

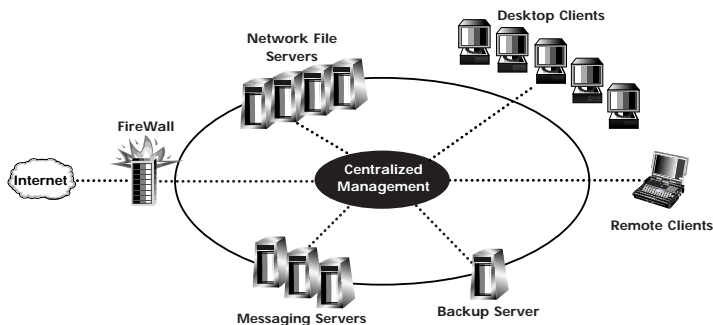
# Deploying Enterprise-wide Virus Protection

ATG's Communications &  
Networking Technology  
Guide Series

This guide has been sponsored by

**CHEYENNE**<sup>®</sup>  
A Division of Computer Associates

# Viruses don't stop at the desktop Neither should your antivirus software.



## INOCULAN

*AntiVirus for the Enterprise*

Because of the changing nature of the enterprise network, viruses have become more prevalent than ever. The use of email, messaging systems, network file servers and the Internet has led to a tremendous increase in the number of viruses today.

While desktop virus protection is necessary, you need to go beyond the desktop to keep your *entire* network virus free.

InocuLAN provides the most advanced virus protection for servers, clients, messaging systems and the Internet. And all of

InocuLAN's components are tightly integrated and easily managed from a single console. So don't put your company at risk by relying on a desktop antivirus product, find out more about the industry's first antivirus solution for the enterprise at [www.cheyenne.com/security](http://www.cheyenne.com/security) or call 1-800-CHEY-INC today.

## Table of Contents

Introduction . . . . .	2
Computer Viruses . . . . .	5
Anti-virus Software. . . . .	11
Enterprise-Wide Virus Protection . . . . .	14
Multi-Level, Comprehensive Virus Protection . . . . .	15
Features of an Enterprise System . . . . .	20
Essential Features of an Enterprise-capable Anti-virus System. . . . .	22
Deploying and Managing Virus Protection. . . . .	24
Conclusion. . . . .	27
Additional Resources . . . . .	27
Glossary of Terms . . . . .	29

### About the Editor...

Gerald P. Ryan is the founder of Connections Telecommunications Inc., a Massachusetts-based company specializing in consulting, education and software tools which address Wide Area Network issues. Mr. Ryan has developed and taught numerous courses in network analysis and design for carriers, government agencies and private industry. Connections has provided consulting support in the areas of WAN network design, negotiation with carriers for contract pricing and services, technology acquisition, customized software development for network administration, billing and auditing of telecommunications expenses, project management, and RFP generation. Mr. Ryan is a member of the Network+ Interop program committee.

This book is the property of The Applied Technologies Group and is made available upon these terms and conditions. The Applied Technologies Group reserves all rights herein. Reproduction in whole or in part of this book is only permitted with the written consent of The Applied Technologies Group. This report shall be treated at all times as a proprietary document for internal use only. This book may not be duplicated in any way, except in the form of brief excerpts or quotations for the purpose of review. In addition, the information contained herein may not be duplicated in other books, databases or any other medium. Making copies of this book, or any portion for any purpose other than your own, is a violation of United States Copyright Laws. The information contained in this report is believed to be reliable but cannot be guaranteed to be complete or correct.

Copyright © 1997 by The Applied Technologies Group, One Apple Hill, Suite 216, Natick, MA 01760, Tel: (508) 651-1155, Fax: (508) 651-1171  
E-mail: [info@techguide.com](mailto:info@techguide.com) Web Site: <http://www.techguide.com>



**CHEYENNE**  
A Division of Computer Associates

# Introduction

---

Along with the arrival of virtually universal telecommunications and networking, organizations and end-users have developed a tremendous sense of unease about network security issues. The growth of extensive inter-company communications, wide scale intra-company networking, and universal Internet access have also heightened awareness of the possibilities of unwelcome intrusions and attacks upon internal networks.

Although much has been said about network espionage, hacker attacks, and other high-profile security issues, the most profound cause for concern comes not from high tech security probes and intrusions, but from the widespread promulgation of viruses. According to recent surveys<sup>1</sup>, viral infections represent the great majority of all security incidents, and have created tremendous problems for businesses of all sizes.

Virus protection for large organizations is a complex and difficult problem because of the combined hurdles of heterogeneous systems and practices, wide-spread use of distributed or client/server systems, and the free exchange of data files via network sharing, e-mail, and the Internet. As enterprise networks grow through the addition of file and backup servers, messaging systems, Internet gateways, management systems, and wildly proliferating client machines, the need for a comprehensive virus-handling strategy becomes even more critical. Of particular importance is the need to implement a system that allows centralized management of all of the client computers sitting on peoples' desks throughout the organization. Increasingly, organizations are becoming aware that the total cost of ownership of these ubiquitous desk top computers has to include a realistic look at the cost to manage and oversee their security component. The

high frequency of attacks combined with a potential lack of consistent company wide practices for updating virus protection software, make it necessary to include centralized management with integrated solutions to really make a difference.

Until recently, viral infections only threatened data residing on storage media, such as hard drives and floppy disks. However, with the emergence of macro viruses, the threat has spread to applications. As of January 1997, approximately 200 macro viruses have been discovered and documented.<sup>2</sup> The great majority of these attack Microsoft Word documents, the rest attack Microsoft Excel, Ami Pro, and Word Perfect files. However, any application that supports a macro language is susceptible to this type of virus. It is estimated that over 90% of all companies have macro viruses resident somewhere in their computing systems. With this level of penetration, it should be obvious that most organizations are severely lacking in their awareness, management, and prevention of virus attacks.

Establishing effective enterprise level anti-virus security is now possible through the deployment of a new anti-virus software system designed specifically for that purpose. This new approach combines a unified, enterprise-wide, management and operations strategy with multiple level, integrated anti-virus software. The most effective of the virus protection software utilities prevents initial infection rather than simply cleaning up after an infection has already occurred. This unified implementation will be the primary solution in organizations requiring an effective, enterprise-wide, anti-virus strategy.

Enterprise-wide anti-virus solutions need a uniform, all encompassing plan, with centralized control, automated virus signature updates, and support for multiple platforms, protocols, and file types.

Effective deployment of enterprise-wide anti-virus software also requires ongoing vigilance and serious

---

<sup>1</sup> Citations from these *Information Week*, Ernst & Young, and the National Computer Security Association (NCSA)

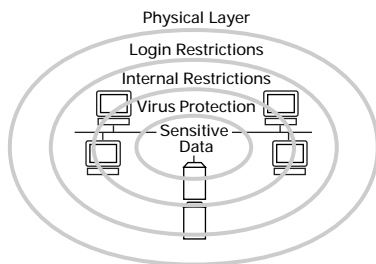
<sup>2</sup> *ibid*

management attention. Although an anti-virus strategy must be supported by technical experts and powerful software, the ultimate responsibility for maintaining a virus-free enterprise ultimately rests on management's shoulders.

This Guide examines various types of security problems that network administrators are likely to encounter, with specific emphasis on viruses and virus protection systems and strategies. It provides a top-down approach to deploying and managing enterprise anti-virus protection systems throughout an organization in a way that assures a high degree of confidence and efficiency.

## The Security Threat

Findings from recent industry studies and surveys indicate that an alarming number of large organizations have failed to implement satisfactory security policies. Furthermore, of the 1,300 companies interviewed in a survey conducted by the National Computer Security Association (NCSA), 54% of the respondents indicated they had experienced significant loss of data due to security breaches, while 78% of these security breaches were directly attributed to virus infection. Reported financial losses of over \$250,000 were common, with losses over \$1 million reported by some enterprises! These statistics clearly indicate that security is an issue that can no longer be ignored, and that viruses are the most common, and unfortunately, the most serious security threats encountered in the workplace.



## Computer Viruses

A computer virus is any program created to reproduce itself. A virus reproduces itself by attaching itself to programs, files, or even to the boot sectors of disks and activates when the infected file or disk is opened or accessed. Once resident in memory, a virus can attach itself to the next file or disk accessed, and so on. A virus may be designed to do harm or simply can have unintended consequences by overwriting other important computer information and causing costly inconveniences to users and network managers.

There are four general types of computer virus.

- File Viruses (including macro viruses), which are attached to files;
- Boot sector viruses in which the boot sectors of floppy or hard disks are infected;
- Master Boot Record (MBR) viruses which infect the disk master boot record; and
- Multi-partite viruses that are a combination of a file virus and a boot sector virus.

## Virus Disguises

As viruses spread, they need to avoid detection in order to succeed in corrupting target computers. Simple viruses, with easily detected signatures are giving way to more sophisticated virus types:

- Polymorphic Virus—Changes its signature, or profile, each time it is activated so that a fixed signature filter will miss it as it does its virus scan.
- Stealth Virus—Attempts to hide their presence by intercepting interrupt services and by feeding back false information to virus protection products and end users.

- Encrypted Virus—Delivered within an encrypted file, undetectable by a simple virus protection scan.

## Alarming Growth Rate

Although as recently as the mid 1980's computer viruses did not exist, their numbers have risen at an alarming rate since then. By the beginning of 1996, close to 5,000 distinct computer viruses had been discovered or created in computer laboratories, while just one year later, at the beginning of 1997, the number was close to 9,000<sup>3</sup>—almost doubling the virus population in a scant year!

Fortunately, the great majority of these viruses were written for research purposes and have never been released into the computer population at large. Of the contemporary documented viruses, less than 300 of them are circulating in the public sphere. These approximately 300 viruses are said to be “in the wild” since they are not under control and are actively spreading to new systems. And of these, only 10 viruses (Word concept, Form, Stealth B/C, Anti-EXE, Monkey, Stoned, Anti-CMOS, NATAS, NYB, and Michelangelo) or their derivatives, are responsible for nearly 95% of all virus infections and subsequent damage to computers.

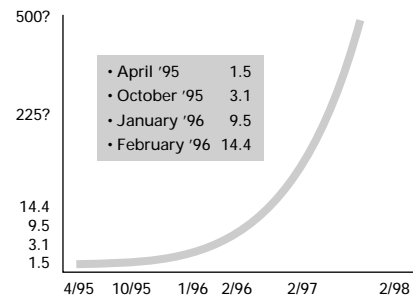
These top10 virus types are responsible for hundreds of millions of lost dollars and countless thousands of lost hours of productivity. And, although these ‘wild’ viruses are a small percentage of the overall virus population, it is in this area that explosive growth is anticipated. Most virus experts agree that we are experiencing the beginning of an explosion of ‘wild’ computer viruses. The reason for this pessimistic forecast is the fairly recent development, and fast spreading epidemic of macro viruses. Any anti-virus solution that fails to protect against 100% of these ‘wild’ viruses

is simply inadequate no matter how many thousands of other tame viruses it does identify and repel.

First discovered in mid-1995, macro viruses are being introduced onto corporate networks and individual workstations at a rapidly increasing rate. By the year 2000, experts say, we will see a dramatic increase in the number of sophisticated viruses and malicious applications circulating throughout corporate networks and individual user workstations.

## Virus Growth Rate

Because of these issues, and as networks grow, the threat of a damaging computer virus infection becomes more likely. According to the NCSA, the threat of contracting a virus is increasing dramatically from its observed 1996 level of 14 infections per thousand computers per month. Ongoing surveys and studies are expected to show infection rates ten times higher in 1997. Studies have also shown that the average cost for diagnosis, cure, and repair of a virus infection has risen to over \$8,000 per incident!



## Sources of Virus Infection

Every new advancement in network and communications technology introduces new avenues through which viruses can infect your system. Most earlier viruses were boot sector viruses, in which the boot sectors of

<sup>3</sup> National Computer Security Association (NCSA)

floppy or hard disks were infected. In fact, as recently as the end of 1995, the only way a machine was likely to be infected by a virus was by using contagious diskettes moved from infected systems to non-infected ones.

## The Spread of Macro Viruses

As stated earlier, the creation of macro viruses has changed this environment dramatically. A macro virus is a set of instructions which is programmed using the powerful macro routines that accompany today's word processing and spreadsheet applications. These macro languages enable a myriad of useful functions to be imbedded into a document which are executed as the document is opened for viewing or use. Primarily targeted at Microsoft Word, which is widely deployed and which contains a rich set of macros, the creators of viruses use these native macros to build their programs. Other word processing and spreadsheet programs, such as Ami Pro and Excel, are also beginning to come under attack.

Surveys conducted by the NCSA indicate that the spread of viruses is accelerating rapidly. Although the figures have not been updated as of this writing, there is convincing evidence that the growth curve implied in these numbers has continued to rise.

## Complicated by the Internet

On its own, this would be a serious problem. But with the exploding development of the Internet, this has catastrophic possibilities. The Internet introduces two different virus threats. The first is caused by downloading files which contain viruses while browsing or using FTP routines; public shareware and executable routines of all types, including formatted presentations are a growing source of virus infection. Furthermore, new Internet virus threats are beginning to appear in the form of malicious JAVA and Active-X applets. The

second major Internet threat comes from e-mail. Most Internet e-mail systems provide a very rich capability to attach formatted documents to e-mail delivered across the network. These e-mail messages can be broadcast to individuals or groups of addressees with the simple stroke of a key! Infected documents or files can be flooded into a corporate network through gateways and mail servers. Imagine a scenario in which a virus attacker obtained the e-mail addresses of an entire corporation and sent a seemingly innocent broadcast message to the entire list, with a macro infected document attached. Most e-mail systems automatically accept attached files and when the recipient opens the document, the virus jumps into his or her computer, ready to re-infect other files.

The simplicity and openness of the network makes this scenario a growing threat. As networking, telecommunications, remote access, message systems that support attachments of all kinds, and interaction with the Internet become more common, viruses will exploit these new electronic pathways to attack systems that were heretofore unreachable.

## Groupware Complications

A third trend in networking also exacerbates the virus threat. This is the trend towards deploying groupware applications such as Lotus Notes, Microsoft Exchange, Novell Groupwise, and Netscape Colabra. Since the active and repeated sharing of documents over the network is at the core of these applications, they represent a fertile ground for the deployment of macro viruses. Groupware software not only acts as a repository for shared documents, but, as an integral part of its collaborative function, simultaneously broadcasts files to associated work groups. This significantly multiplies the possibility of accidentally deploying infected mail through attached macro viruses and makes groupware protection a high priority.

## Symptoms of Virus Infection

Most viruses attempt to remain undetected as long as possible so they can extend their often destructive influences. Therefore, through the use of these three techniques, most viruses do not produce any recognizable profile or signature that would allow scanning software to trap them. However, viruses do perform actions that do not resemble normal computer or user operations and these actions can be detected by intelligent anti-virus software. Fortunately, many viruses have telltale symptoms and inadvertently give off signals that can alert users and virus protection software to their presence. Some of these symptoms include:

- Increase in byte length of files,
- Alterations of a file's time stamp,
- Delayed program loading or activation,
- Reduced system performance,
- Lower system resources, available memory, disk space,
- Bad sectors on floppies and hard drives,
- Strange or non-standard error messages,
- Non-standard screen activity, display fluctuations,
- Program inoperability (failing to execute),
- Incomplete or failed system boots, and
- Uninitiated drive writes.

In an extreme case, the virus may trigger a disaster in which the system is completely disabled and there is a loss of access to critical data. If one or more of these symptoms occurs, it may signify the presence of a virus. In the next section, we discuss the characteristics of anti-viral software that has been designed to notice such virus symptoms, and that can initiate remedial measures to clean up and protect systems where such symptoms occur.

## Anti-Virus Software

---

### Detecting a Virus

When choosing effective anti-virus software, it is essential that it have a varied and multi-faceted array of methodologies for fighting viruses. Contemporary viruses are becoming increasingly sophisticated and, as such, can defeat simpler, single dimension software packages. To be effective, the anti-virus software utility must include special-purpose, distributed applications that can detect viruses using five distinct methods.

- **Signature Scanning:** Compares the content of files against a database of virus signatures. This requires a frequent database update to assure that new and changing signatures are identified.
- **Integrity Checking:** Compares the profile of current files and disk areas against an archived snap shop of these same items. Differences that are detected may indicate the presence of a virus. Check summing is the most common type of integrity checking. Unfortunately, integrity checking is generally not effective against modern stealth viruses, so other approaches are needed as well.
- **Heuristic Analysis:** In which artificial intelligence monitors for virus-like behavior, such as trapping certain interrupt services or attempting unlikely actions such as reformatting the hard disk.
- **Polymorphic Analysis:** Polymorphic viruses are difficult to detect because they constantly change the way they look, particularly when they are also encrypted or use stealth techniques to hide their presence. A polymorphic analyzer will move any suspect file to a separate, protected,

location in the computer and execute it there to see if it exhibits any virus-like behavior.

- **Macro Virus Analysis:** A specifically designed anti-virus software that detects macros in files before execution and tests them for viruses.

## Archived and Compressed Files

In addition to supporting these five types of analysis, effective anti-virus systems must also be able to scan archived and compressed file types. The most common such types include zip (or Pkzip) and Microsoft Compression. Viruses can hide inside such compressed archives, and remain dormant or unnoticed until infected files are extracted and released into a system. At a minimum, an anti-virus system should be able to scan most archive types to identify viruses stored within any files they contain.

## NCSA Certification

The National Computer Security Association (NCSA) provides comprehensive and objective oversight to the anti-virus industry and provides a clearing house of information regarding emerging or changing viruses. It provides a formal certification process in which it evaluates and rates anti-virus software on a regular basis. This certification is conducted on a year to year basis and includes bi-monthly rechecking of the software throughout the certification year. For the tested anti-virus software to pass the certification process, it must be able to detect 100% of the viruses on the current 'wild' list as well as 90% of the 9,000+ known viruses.

## Frequency of Database Signature Update

Ultimately, any anti-virus software's ability to actively prevent virus attacks will be determined by the currency of its database of virus signatures. Any anti-

virus software worth deploying must have an associated, easily accessible Web site, or some other online source of information, where regular virus database updates can be retrieved. Those products that automate this update process by using a network's Internet connection to routinely poll for new database information have a clear advantage in this regard.

## Curing a Virus

Most anti-virus software can not only detect, locate, and identify viruses, but can also remove viruses from an infected system. The removal process may be unique to each virus, but can include the deletion of virus code, the repair of damaged files, and may sometimes even apply patches to damaged applications.

## Virus Scanning: Real Time and Scheduled

Most anti-virus software can perform a scan of a computer detecting, and even repairing, all viruses found at that time. This process is called scanning. Scanning a computer for viruses on a scheduled basis can occur at regular intervals as determined by a system's scheduler, or as an on-demand operation that's manually executed, or as an event-activated operation (usually in response to some recognizably "illegal" behavior by a potential virus).

In addition, viruses can be scanned in real time, i.e., as they are received into the computer, data repository, or server. This is an important capability because if viruses can be detected as they attempt to enter a system, then they can be prevented from corrupting any files. Oftentimes, a scheduled scan may occur after a virus has already entered a computer and has had an opportunity to corrupt other files. Obviously, the earlier a virus can be detected, the better.

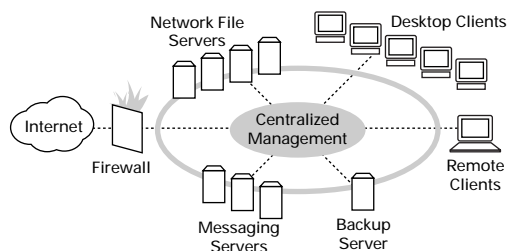
For anti-virus software to be truly useful, it must have the ability to perform all types of scans.



## Management Issues

Because of the complexity of corporate networks and the reality of inconsistent human behavior, managing a network anti-virus system introduces surprisingly difficult problems. One major concern is the currency of the anti-virus software and its uniform deployment throughout the corporate enterprise. A key element in providing consistency in an enterprise-wide anti-virus system is the ability to uniformly and automatically deploy software updates in a timely and controlled way. This managerial capability is essential to a successful deployment. Other important management features of virus protection software include report generation, logging of all virus-related activities, and centralized management of distributed protection systems. Administrators will ultimately need all of these capabilities in the continuing war against computer viruses.

## Enterprise-Wide Virus Protection



Virus protection within an enterprise demands a significantly more robust solution than that which is required for stand-alone computers or small networks.

An enterprise network consists of many levels of functionality. Generally based on LAN architectures which are interconnected through switches to e-mail and file servers and which are then connected to the world via routers and gateways, these networks have a number of unique issues.

## Multi-Level, Comprehensive Virus Protection

Of overriding concern is the question of where anti-virus software should be deployed. Within a corporate enterprise, critical data is most often stored on networked file servers located centrally and throughout the network fabric. These file servers are the primary target of viruses aimed at corporate users. To protect them, corporate managers must provide comprehensive protection at many levels of the network.

It is important to recognize that the best protection involves a multi-level solution that enable four key attributes:

- **Integration:** The solution includes a deliberately coordinated approach that integrates all of the layers of protection within a single paradigm.
- **Single Point Management:** As an essential element of an integrated solution there should be a single focal point of security management.
- **Automation:** The solution should include the ability to automatically update virus signatures and other anti-virus elements.

- **Multi-layered:** The solution should be multi-layered in that the right components are distributed at the most effective point to maximize efficiency and reduce overhead. Anti-virus software needs to be installed in servers, workstations, and messaging systems.

## Gateways and Firewalls

Some suggest that it makes sense to put all anti-virus software right at the gateway to prevent any viruses from even entering the network. This approach, however, has two major problems. The first is the problem of severe performance degradation. Gateways, or routers, and even routers, are designed to read a header on a frame or packet and then pass the frame or packet along to its destination as quickly as possible. In order to check for viruses, the router or gateway would have to receive all of the frames of the file, reconstruct them, and store them temporarily while a scan takes place. This is completely opposite of the desired effect. The performance of the router or gateway would degenerate very quickly causing severe bottlenecks in and out of the network.

## Workstations

The essential element is to have the anti-virus software reside right on each workstation in the network since this is the main entry point into the network. This approach makes great sense because the scanning workload is shared among all of the computers in the system, putting only a small workload overhead on each station. Each station would be equipped with up-to-date anti-virus software and could add this task to its ordinary workload with little performance degradation and no need for new equipment. Although a growing number of virus infections today stem from Internet downloads and e-mail attachments, still the most common source of

infection is from floppy diskettes brought in from employees homes. Real-time floppy scanning needs to be done on the workstation to keep virus infections down, as the workstation is the most common virus entry point. The caveat, of course, is that the software has to be part of a system that enforces uniform updates and automatic operation so as to avoid user inconsistencies.

## E-mail Servers

E-mail servers are a second natural location for anti-virus scanning. Since all of the e-mail messages, which are a primary source of infection, come into the servers and are archived in mailboxes before being sent on their way, it makes great sense to include anti-virus software on them. With a ratio of about 100:1 workstations to mail servers, the cost efficiency of this solution makes sense. Unfortunately, this does not cover all of the ways in which viruses can come into individual workstations. With separate modems connected to the Internet, and with direct connection to other stations in the network, corporate mail servers can be bypassed; which is why, it is important to cover all other entry points.

## Backup Servers

Backup servers are responsible for maintaining copies of critical data. If backup files are corrupted, then the system is fundamentally flawed. Corrupted files may be unusable for restoral purposes or may re-infect entire systems. A little known issue with anti-virus software is that it generally conflicts with backup software. Backup software, as part of its ordinary operation, opens up files multiple times as part of its process. This requires the anti-virus software to scan these same files multiple times. A major backup system which could support, for example, 50,000 files. During an overnight backup process, virus checks are conducted as many as

150,000 times! Creating tremendous slowdowns and inefficiencies. This is complicated by the fact that when a virus is detected, the system stops until the virus infection is cured. This means that a backup would have to be conducted the next day, rather than as an overnight process. Therefore, it is critical that an effective software product be installed that is designed to overcome this inconsistency. Protecting backups from virus infestation is integral to maintaining a safe and secure network. Good anti-virus software must collaborate with backup software to provide real-time backup and restoration virus protection.

## Internet Servers and File Servers

Anyplace in the network where a file or database resides is a potential source of problem. It is essential that these locations are well protected. A file server houses a company's most critical data. And, having your Internet server equipped with anti-virus software is of paramount importance. Keeping files uploaded and downloaded virus free is important to your network and your customer's network.

## The Overall Architecture

An enterprise solution therefore, requires anti-virus software installed in mail servers, file archive systems, and workstations. In addition, this multi-tiered array of software protection requires a management scheme to control it and ensure its success.

## The Human Factor

It is a fact that the vagaries of human behavior would lead to an uneven application of anti-virus software, if the decision and responsibility to install and use anti-virus software resided with each workstation user. Most people in an uncoordinated, free standing

environment, have some form of anti-virus software, but it is often outdated and, because it is often times a consuming and fruitless task to use it, it falls into disuse. As a result, there is a need to have a system that enforces and enables the easy updating and regular use of such software.

To reach this goal, an anti-virus product must have strong central management features (including the ability to interact and integrate with any existing management scheme already in place), a high level of automated functionality (including virus signature updates, infestation notification, detection, cure, and clean-up, and detail log reporting), as well as enterprise-wide, consistent, automatic event-triggered virus protection, detection, and cure.

Enterprise virus protection systems must have a scheme in which network administrators can compel user compliance. This will prevent ordinary users from subverting the system by turning off automated protection, and enabling mandatory virus scans throughout an enterprise network. Furthermore, the authority can mandate that every file, whether public, private, or system-level be regularly inspected for virus activity. Central management of anti-virus software also aids in reducing administrative time and frustration by including the ability to update all virus databases from a single location, and to customize scanning parameters for each system throughout an enterprise. The ability to manage multiple machines, yet limit related network traffic, is likewise essential (to keep the cure from being worse than the disease).

The ability of anti-virus software to detect numerous viruses is not the only true measure of its effectiveness. Such software's true effectiveness also lies in its ability to prevent virus infestations, in its oversight with large numbers of files, drives, and systems, and finally, in its facilities to alert administrators about possible infestations and virus origins.

# Features of An Enterprise System

---

Relevant features in enterprise-ready anti-virus software must therefore include the following capabilities.

## Domain Management

For an enterprise anti-virus system to be truly effective, it must be able to manage an entire domain of hundreds or thousands of nodes (servers and workstations) as a single entity. The product's management facilities must be aware of all potential virus activity on each computer, and at each entry point to the network. The key to maintaining control over an entire domain is centralized administration and management. One (or a few) computer(s) should host an anti-virus system's control application, where system wide or single node changes can be applied to anti-virus information, configuration, and behavior at will.

## Quarantine and Source Tracking

A second aspect of complete domain management is an anti-virus solutions ability to isolate infected clients. When a node's protection scheme identifies a potential infection, the central control facility should be able to terminate its network access. This prevents a virus from spreading through the network. Once all infected computer(s) are quarantined, the anti-virus system's management facility notify its administrator(s) of the need for immediate action.

Intelligent anti-virus software should also be able to identify the infected computer and the user logged into the computer. This permits specific clients or roaming users to be identified as repeat offenders. A trail of

evidence can be supplied by the virus tracking system automatically and, if necessary, this data can be used to support a case for legal action against the responsible individual(s), as well as providing a useful method to identify and diagnose sources of infection.

## Alarms and Alerts

Enterprise administrators must be notified when a virus outbreak occurs.

The anti-virus system's alarms and notifications should have a wide range of customizable options, such as setting virus activity notification levels, identifying selected administrators or managers when problems occur, and variable levels of text messages for event logs. The process of notification should include e-mail, on-screen alerts to designated recipients, alphanumeric or digital pages (with codes to identify alarm urgency), simple event log entries, automatic printouts of virus trouble tickets and Interfacing with SNMP based network management systems. These alarms and alerts must be integrated with the overall system management architecture.

## State of the Art Virus Identification

Anti-virus software must be able to identify a wide range of virus types. Each type possesses unique difficulties relating to its identification, inoculation, and repair, and each will be detected or identified through different means. Whatever anti-virus product you deploy in your enterprise must support methods to detect each of these types, and be able to accommodate new virus types or detection methods as they are introduced.

# Essential Features of an Enterprise-capable Anti-virus System

---

The following is a list of bottom-line requirements that an anti-virus software solution must have to provide sufficient protection for an enterprise network.

- NCSA Certification—anti-virus software must be certified to detect 100% of current viruses in the wild.
- Detect and Cure Viruses—in Real-Time.
- Administrative Tools—Domain management and virus event tracking, etc. across multiple servers and workstations.
- Single Management Console.
- Automatic Installation and Updates.
- Easy to use Graphical User Interface.
- Prevent infected workstations from copying viruses onto servers.
- Tracks source of virus infection.
- Quarantines infected workstations.
- It should allow the rest of the system to continue running after a virus is detected and isolated and cured.
- Automatically update virus signatures monthly on all clients and servers.
- Compatibility with popular Internet browsers.

- Act as a client for server based anti-virus software.
- Compatibility with existing SNMP-based management systems.
- Compatibility with centralized management platforms like CA Unicenter and HP Openview.
- Have virus wall to prevent writing viruses to servers.
- Operation over, through, or behind firewalls, proxies, and remote hosts.

Other aspects that are important to a solid barrier of virus protection include:

- No human intervention required. Anti-virus software must operate whether or not a human is present. Automating the detection, curing, and repair processes will elviate the problem of relying on a person to perform the tasks of initiating virus scans and cures.
- Non-Interfering Operation. Anti-virus software needs to be transparent to users, in other words use little memory, execute quickly, and keep system load to a minimum and be automatically updated. The barrier is to prevent virus activity, not reduce the productivity of users.
- Multilayered. For a solution to be effective, the core modules must be able to be expanded or extended through additional components designed to add protection to specific areas at point of entry. Protection has to populate workstations, servers, and messaging systems.

# Deploying and Managing Virus Protection

---

The actual deployment of a virus protection tool commonly requires completing the following steps:

1. **Planning.** Determine what types of information or data feeds are present on your network.
2. **Research.** Identify a software solution that fits all your assessed needs, plus as many of the features listed in the preceding baseline checklist.
3. **Testing.** With a limited group, install and test the operation of the software, to make sure it works properly, and is compatible with existing networking and applications software.
4. **Maintain.** Manage and update the software to ensure that it functions as expected, and that it's possible to manage using your current network and staff; be sure to download updates and signature files, and apply them to your test network, to fully understand this crucial aspect of any anti-virus system.
5. **System Deployment.** Once satisfied with a product, deploy it system wide.

## Continuous Virus Protection

The continuous operation of virus software, no matter how automated a package claims to be, requires consistent administration and oversight. No virus solution should require 24/7 hands-on supervision to be effective. However, you should be apprised of the status of all virus activity throughout an enterprise, and understand the level of administration that's required to maintain your desired level of virus protection. Developing such an understanding will require one of more of the following activities:

- Integration with company security policies, prior to first-time deployment, and as company policies change.
- Immediate installation of software upgrades, as available.
- Manual inspection of suspect objects or events, as soon as possible after detection.
- Ongoing evaluation of the costs of ownership.
- Continued vigilance against viruses, and ongoing management of the ever-changing set of components that will comprise most acceptable anti-virus systems.
- Educate end users.
- Change the boot sequence in the CMOS of all computers.
- As in any protection scheme, your barrier is only as reliable as the weakest link. Be proactive in testing and strengthening each aspect of your defense system.

## Developing an Anti-virus Policy

Many organizations have learned that simply installing an anti-virus product on their system fails to effectively safeguard their network from infection. Generally, the oversight involved is two fold if the software installed is inadequate, and its administrators have not learned how to properly apply its protection schemes. One solution is a well-crafted company policy that clearly defines how virus protection should be established and maintained. The following six items are essential to establishing a real-world virus policy and ultimately to erecting a reliable barrier against infection.

1. **Focus on Software.** Virus protection ultimately rests on the quality of the software that's deployed. Attempting to alter or control user

- behavior, no matter how motivated and dedicated, is futile.
2. **Response Team.** A team of two or more people trained in proper handling of virus infections is an essential element of a complete protection policy.
  3. **Automated Prevention.** Every user must run an intelligent anti-virus protection tool at all times.
  4. **Upgrades and patches.** The best protection is the latest version of your anti-virus system. Every upgrade, patch, or update to your anti-virus software should be downloaded, tested, and rapidly deployed. It is essential that the anti-virus system has the facility to automate this process to eliminate the vagaries and whims of individual human behavior.
  5. **Always have a Backup.** Protect your data and your system by maintaining a reliable, current, virus-free backup. In the event of virus disaster, you will be able to restore your system quickly.
  6. **Virus-free servers.** The central focus of a network is its file servers, where data and services are stored and accessed. These valuable resources must be reliably protected. Once a server is compromised, your entire network is at risk. Your policy should be to protect servers from viruses at all costs.
  7. **Identify Risk-Takers.** Users who repeatedly expose your network to viruses, perform a lot of data transfers from outside sources, or attempt to bypass anti-virus barriers should be reprimanded and possibly relieved of their network privileges. Be aware that other high-risk users, such as repair technicians, contractors, consultants, and salesmen, who may be unaware of your virus policies or rigid protection barriers, are also prime potential sources of infection.

8. **No Unapproved Software.** Eliminate uncontrolled sources of software, and you effectively reduce virus infection, piracy, and support problems.

---

## Conclusion

Enterprise-wide virus protection is a necessary and critical part of today's network environment. It is as much a strategy or an attitude as it is a collection of information and software. It demands a comprehensive centralized control, automated signature updates, and statistics reporting, and must support multiple platforms, protocols, and file types.

Because of the increasing complexity of communications both within an organization and between organizations, effective deployment of enterprise-wide anti-virus software requires ongoing effort. Although an anti-virus strategy must be supported by powerful software, the ultimate responsibility for maintaining a virus-free enterprise rests on its network administrators. A comprehensive anti-virus software solution with truly integrated multi-layer (performance) will solve the problems long associated with network viruses.

---

## Additional Resources

For more information about viruses and the deployment of anti-virus software please visit the following resource sites:

- "Virus Prevention Policies that Work," by David Stang—  
<http://www.cheyenne.com/security>

- The National Computer Security Association (NCSA)—  
<http://www.ncsa.com/>
- Virus Research Unit of the University of Tampere, Department of Computer Science—  
<http://www.uta.fi/laitokset/virus/>
- “Virus Bulletin: the international publication on computer virus prevention, recognition and removal”—  
<http://www.virusbtn.com/>
- “Computer Virus Myths,” by Rob Rosenberger—  
<http://kumite.com/myths/>
- The Original J and A Computer Virus Information Page—  
<http://www.bocklabs.wisc.edu/~janda/>
- Cheyenne’s Security Center—  
<http://www.cheyenne.com/security>
- AVP Virus Encyclopedia—  
<http://www.metro.ch/avpve/>
- U.S. Department of Energy’s Computer Incident Advisory Capability—  
<http://ciac.llnl.gov/ciac/>
- USENET FAQs for comp.virus—  
<http://www.cis.ohio-state.edu/hypertext/faq/bngusenet/comp/virus/top.html>

## Glossary

---

**Administration Management Domain (ADMD)**—An X.400 Message Handling System public carrier. Examples: MCIEmail and ATTmail in the U.S., British Telecom’s Gold400mail in the U.K. The ADMDs in all countries worldwide together provide the X.400 backbone.

**Administrative Domain (AD)**—A group of hosts, routers, and networks operated and managed by a single organization. This Internet concept is defined in RFC 1136.

**Advanced Intelligent Network (AIN)**—Carrier offering more than “pipes” to users.

**Advanced Peer-to-Peer Networking (APPN)**—IBM SNA facility that provides distributed processing based on Type 2.1 network nodes and Logical Unit (LU) 6.2.

**Agent**—In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. In SNMP, the word agent refers to the managed system.

**Audit Trail**—Audit trails provide a date and time stamped record of the usage of a system. They record what a computer was used for, allowing a security manager to monitor the actions of every user, and can help in establishing an alleged fraud or security violation.

**Authentication**—(1) The process of determining the identity of a user who is attempting to access a system. (2) The process of assuring that data has come from its claimed source, or of corroborating the claimed identity of a communicating party.

**Auto Open**—An optional feature which Opens a Field by pressing ENTER, running a Field Command.



**Automatic Protection Switching (APS)**—The ability of a network element to detect a failed working line and switch the service to a spare (protection) line. 1 +1 APS pairs a protection line with each working line. 1:n APS provides one protection line for every n working lines.

**Backup**—A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

**Bad Sectors**—During formatting of MS-DOS disks, all sectors are checked of reusability. Unusable sectors are labeled as bad and are not used by DOS. The remaining areas can then still be used. Viruses sometimes label good sectors as bad to store their code outside the reach of users and the operating system.

**Bandwidth**—(1) Measure of the information capacity of a transmission channel. (2) The difference between the highest and lowest frequencies of a band that can be passed by a transmission medium without undue distortion, such as the AM band—535 to 1705 kilohertz. (3) Information carrying capacity of a communication channel. Analog bandwidth is the range of signal frequencies that can be transmitted by a communication channel or network.

**Bits Per Second (bps)**—The number of bits passing a point every second. The transmission rate for digital information.

**Boot Sector Virus**—A type of computer virus which subverts the initial stages of the bootstrapping process. A boot sector virus attacks either the master bootstrap sector or the DOS bootstrap sector of a disk.

**Bootstrap Sector**—Part of the operating system which is first read into memory from disk when a PC is switched on (booted). The program stored in the bootstrap sector is then executed, which in turn loads the rest of the operating system into memory from the system files on disk.

**Broadcast**—(1) A message sent to all network destinations. (2) To send or transmit by radio or television.

**Broadcast Address**—A special address that is reserved for simultaneous broadcast to all stations.

**Broadcast Domain**—Defines the set of all devices which will receive broadcast frames originating from any device within the set. Broadcast domains are normally bounded by routers.

**Broadcast Storm**—Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network time-outs.

**Broadcast Storm Firewalls**—A mechanism that limits the rate at which broadcast/multicast packets are forwarded through the system.

**Browser**—Term used to describe the client program for the World-Wide Web. Popular browsers include Mosaic and Netscape. Sometime called “navigator.”

**Buffer**—A storage area used for handling data in transit. Buffers often are used to compensate for differences in processing speed between network devices.

**Buffer Allocation Size (BA Size)**—Number of octets in L3-PDU from DA to Info, +CRC if present (SMDS).

**Bus Topology**—Linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations attached to the medium.

**Bypass Mode**—Operating mode on FDDI and Token Ring networks where an interface has de-inserted from the ring.

**Byte**—Generic term used to refer to a series of consecutive binary digits that are operated upon as a unit; for example, an 8-bit byte.

**Byte-Interleaved**—Bytes from each STS-1 are placed in sequence in a multiplexed or concatenated STS-N signal. For example, for an STS-3, the sequence of bytes from contributing STS-1s is 1,2,3,1,2,3...

**Caching**—Speeds information processing by storing information from a transaction to use for later transactions.

**Checksum**—A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered. Usually 32 or 64 bits long

**Client**—The part of Staffware which Users interact with.

**Client/Server**—A distributed system model of computing that brings computing power to the desktop, where users (“clients”) access resources from servers.

**Commercial Internet Exchange (CIX)**—A connection point between the commercial Internet service providers. Pronounced “kicks.”

**Companion Virus**—A virus which “infects” EXE files by creating a COM file with the same name and containing the virus code. They exploit the MS-DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

**Complementary Metal-Oxide Semiconductor (CMOS)**—Is a technology used to manufacture chips which have very low power consumption. CMOS chips are used in battery-backed applications such as the time-of-day clock and for the non-volatile storage of parameters in IBM-ATs.

**Computer Emergency Response Team (CERT)**—The CERT is chartered to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proac-

tive steps to raise the community’s awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

**Congestion**—Excessive network traffic.

**Cryptographic Checksum**—A one-way function applied to a file to produce a unique “fingerprint” of the file for later reference. Checksum systems are a primary means of detecting file system tampering on UNIX.

**Cyclic Redundancy Check (CRC)**—A mathematical method for verifying the integrity of data. It is a form of checksum, based on the theory of maximum length polynomials. While more secure than a simple checksum, CRCs do not offer true cryptographic security. See cryptographic checksum.

**Data Compression**—Reducing the size of a data file by reducing unnecessary information, such as blanks and redundant data.

**Data Driven Attack**—A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

**Data Encryption Standard (DES)**—A popular, standard encryption scheme.

**Data Exchange Interface (DXI)**—(1) ATM: A variable-length frame-based ATM interface between a DTE and a special ATM DSU/CSU. The ATM DSU/CSU converts between the variable-length DXI frames and the fixed-length ATM cells. (2) Defines the format for transmitting information that has gone through the ATM convergence sublayer.

**Data Protection**—A group of techniques used to preserve three desirable aspects of data: confidentiality, integrity, and availability. Also a legal term with specific meaning (somewhat different to the above definition.)

**Dedicated Access**—A leased, private connection between a customer's equipment and a phone company location, most often that of an interexchange carrier.

**Dedicated LAN**—Network segment allocated to a single device. Used in LAN switched network topologies.

**Defense Data Network (DDN)**—Comprises the MILNET and several other DoD networks.

**Defense Information Systems Agency (DISA)**—The new name for DCA.

**Descrambler**—An electronic circuit that restores a scrambled video signal to its standard form.

**Digital Signature**—A means of protecting a message from denial of origination by the sender, usually involving the use of asymmetric encryption to produce an encrypted message or a cryptographic checkfunction.

**Distributed Computing Environment (DCE)**—An architecture of standard programming interfaces, conventions, and server function personalities (e.g., naming, distributed file system, remote procedure call ) for distributing applications transparently across networks of heterogeneous computers. Promoted and controlled by the Open Software Foundation (OSF), a vendor consortium.

**DNS Spoofing**—Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

**Domain**—In the Internet, a part of a naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by

periods (dots), e.g., "tundra.mpk.ca.us." In OSI, "domain" is generally used as an administrative partition of a complex distributed system, as in MHS Private Management Domain (PRMD), and Directory Management Domain (DMD).

**Domain Name System (DNS)**—The distributed name/address mechanism used in the Internet.

**Dynamic Bandwidth Allocation (DBA)**—A process that optimizes overall network efficiency by automatically increasing or decreasing the bandwidth of a channel to accommodate changes in data flow from end-user equipment.

**Dynamic Data Exchange (DDE)**—This is a method of transferring data between two Windows applications while they are running

**Dynamic Password Authentication Servers**—Products consisting of server software that generates constantly changing passwords and two-factor, software or hardware-based password generators that teleworkers carry with them.

**Encryption**—Applying a specific algorithm to data so as to alter the data's appearance and prevent other devices from reading the information. Decryption applies the algorithm in reverse to restore the data to its original form.

**End User**—Any customer of an interstate or foreign telecommunications service that is not a carrier, except that a carrier other than a telephone company shall be deemed to be an "end user" when such carrier uses a telecommunications service for administrative purposes. It is also a person or entity that offers telecommunications services exclusively as a reseller shall be deemed to be an "end user" if all resale transmission offered by such reseller originate on the premises of such reseller.

**Enhanced Monitoring Services (ENS)**—The Catalyst Enhanced Monitoring Services consist of an integrated RMON agent and Switched Port Analyzer (SPAN). These two analysis tools allow the monitoring of traffic across all eight Ethernet ports on the Catalyst Switch. Network segments can be selectively managed and analyzed.

**Enterprise Network**—A geographically dispersed network under the auspices of one organization.

**Error-Detecting Code**—A code in which each data signal conforms to specific rules of construction, so that departures from this construction in the received signal can be automatically detected.

**Ethernet**—A baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks operate at 10 Mbps using CSMA/CD to run over coaxial cable. Ethernet is similar to a series of standards produced by IEEE referred to as IEEE 802.3.

**Extended Industry Standard Architecture (EISA)**—A standard bus interface, commonly used by PCs and some UNIX workstations and servers.

**Exterior Gateway Protocol (EGP)**—(TCP/IP) The service by which gateways exchange information about what systems they can reach; generally, an exterior gateway protocol is any internetworking protocol for passing routing information between autonomous systems.

**False Negative**—An existent event reported as non-existent, e.g. a virus failing to be detected.

**False Positive**—A non-existent event reported as existent, e.g. a virus being reported when no virus is present.

**Fault Tolerance**—Generally, the ability to prevent a problem on a device from affecting other devices on the same port.

**Federal Internet Exchange (FIX)**—A connection point between the North American governmental internets and the Internet. The FIXs are named after their geographic region, as in “FIX West” (Mountain View, California) and “FIX East” (College Park, Maryland).

**Field Command**—A Staffware Command, usually a function call or assignment, which is performed when the Field is Opened.

**File**—A program, document, or data stored on a disc or tape with an identifying name.

**File Transfer Protocol (FTP)**—An IP application protocol for transferring files between network nodes.

**File Transfer, Access, and Management (FTAM)**—The OSI remote file service ad protocol.

**Filter**—Generally, a process, or device that screens incoming information for certain characteristics, allowing a subset of that information to pass through.

**Firewall**—Isolation of LAN segments from each other to protect data resources and help manage traffic.

**Flooding**—Technique by which information received by an internetworking device is sent out to each of the device’s interfaces except (usually) the interface on which the information was received.

**Footprint**—The area in which a satellite’s transmission can be received. Some footprints cover as much as one-third of the earth.

**Frame**—A logical grouping of information sent as a link-layer unit over a transmission medium. The terms packet, datagram, segment, and message are also used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

**Frame Relay**—High-performance interface for packet-switching networks. Considered more efficient

than X.25 which it is expected to replace. Frame relay technology can handle “bursty” communications that have rapidly changing bandwidth requirements.

**Frame Relay Forum**—A voluntary organization composed of Frame Relay vendors, manufacturers, service providers, research organizations, and users. Similar in purpose to the ATM Forum.

**Frame Switch**—A device, similar to a bridge, which forwards frames based on the frame’s layer 2 address. Frame switches are generally of two basic forms, cut-through switch (on the fly switching), or store and forward switch. LAN switches such as Ethernet, Token Ring, and FDDI switches are all examples of frame switches.

**Frequency Modulation (FM)**—Radio transmission covering 88-108 megahertz on the broadcast band. It is less susceptible to interference than AM broadcasting. Also used in other frequency bands for two way communications in land mobile and marine services.

**Functional Group**—A set of functions that may be performed by a single piece of equipment.

**Gateway**—A set of functions intended to facilitate electronic access by users to remote services and vice versa. Gateways are intended to provide a single source through which users can locate and gain access to a wide variety of service. Gateways typically offer a directory of services available through them, and provide billing for these services.

**Gateway Daemon (GateD)**—A popular routing software package which supports multiple routing protocols. Developed and maintained by the GateDaemon Consortium at Cornell University.

**Gigabits Per Second (Gbps)**—Billion bits per second. A measure of transmission speed.

**Global Internet Exchange (GIX)**—A common routing exchange point which allows pairs of networks to implement agreed-upon routing policies. The GIX is intended to allow maximum connectivity to the Internet for networks all over the world.

**GUI**—Graphic User Interface.

**Heart Beat**—A transmission sent by a transceiver back to the controller to let the controller know whether the collision circuitry is functional.

**Heterogeneous LAN management (HLM)**—OSI NMS protocol specification without layers 3-6 developed by IBM and 3Com to save memory in workstations.

**Hierarchical Routing**—Routing based on a hierarchical addressing system. IP routing algorithms use IP addresses which contain network numbers, host numbers, and frequently, subnet numbers.

**High Performance Parallel Interface (HIPPI)**—An emerging ANSI standard which extends the computer bus over fairly short distances at speeds of 800 and 1600 Mb/s. HIPPI is often used in a computer room to connect a supercomputer to routers, frame buffers, mass-storage peripherals, and other computers.

**High Performance Routing (HPR)**—A form of dynamic call routing in the PSTN.

**High Speed Data (HSD)**—DTE interface normally using V.35 or EIA530 standards.

**High Speed Data Link Control (HDLC)**—A protocol defined by the International Standards Organization and used in X.25 communications. It specifies an encapsulation method for data on synchronous serial data links. Various manufacturers have proprietary versions of HDLC, including IBM’s SDLC.

**High-Speed Peripheral Parallel Interface (HIPPI)**—Computer channel simplex interface clocked at 25 MHz; 800 Mbit/s when 32 bits wide, 1.6 Gbit/s when 64 bits.

**Host**—The term used in the Internet community to describe any device attached to the network which provides application level service (i.e., a machine that you can log in to and do useful work.) A router is not a host.

**Hub**—Common name for a repeater. Strictly, it is a non-retiming device.

**Hyper Text Transfer Protocol (HTTP)**—The protocol most commonly used in the World-Wide Web to transfer information from Web servers to Web browsers.

**Insider Attack**—An attack originating from inside a protected network.

**Integrity**—A security protection aimed at ensuring that data cannot be deleted, modified, duplicated or forged without detection.

**Internet**—A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network.

**Internet Address**—Also called an IP address. It is a 32-bit address assigned to hosts using TCP/IP. The address is written as four octets separated with periods (dotted decimal format) that are made up of a network section, an optional subnet section, and a host section.

**Internet Assigned Numbers Authority (IANA)**—The entity responsible for assigning numbers in the Internet Suite of Protocols.

**Internet Control Message Protocol (ICMP)**—A network-layer Internet protocol that provides message packets to report errors and other information relevant to IP packet processing. Documented in RFC 792.

**Internet Protocol (IP)**—A Layer 3 (network layer) protocol that contains addressing information and some control information that allows packets to be routed. Documented in RFC 791.

**Internet Service Provider (ISP)**—Any of a number of companies that sell Internet access to individuals or organizations at speeds ranging from 300bps to OC-3.

**Internetwork**—A collection of networks inter connected by routers that function (generally) as a single network. Sometimes called an internet, which is not to be confused with the Internet.

**Internetwork Packet Exchange, Network Protocol (IPX)**—LAN protocol developed by Novell for NetWare.

**Internetworking**—General term used to refer to the industry that has arisen around the problem of connecting networks together. The term can refer to products, procedures, and technologies.

**Intrusion Detection**—Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

**IP Datagram**—The fundamental unit of information passed across the Internet. Contains source and destination addresses along with data and a number of fields which define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

**IP Splicing/Hijacking**—An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

**IP Spoofing**—An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

**ISDN Terminal Adapters**—Simple devices that provide ISDN compatibility by connecting an ISDN line to the serial port of a personal computer.

**Java**—A programming language developed by Sun Microsystems. Applets written in Java include their own software players, so you can download and run them on any computer.

**Kerberos**—A component of MIT's Project Athena. Kerberos is the security system, based on symmetric key cryptography.

**LAN Emulation**—A technique for legacy LAN MAC-layer protocols like Ethernet and token ring, to work transparently across an ATM network.

**LAN segmentation**—Dividing LAN bandwidth into multiple independent LANs to improve performance.

**Listserv**—An automated mailing list distribution system originally designed for the Bitnet/EARN network. Listserv allows users to add or delete themselves from mailing lists without (other) human intervention.

**Local Area Network (LAN)**—(1) A network covering a relatively small geographic area (usually not larger than a floor or small building). Compared to WANs, LANs are usually characterized by relatively high data rates. (2) Network permitting transmission and communication between hardware devices, usually in one building or complex.

**Logic Bomb**—A program modification which causes damage when triggered by some condition such as the date, or the presence or absence of data e.g. a name.

**Mail Gateway**—A machine that connects two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be quite complex, and generally it requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

**Mapping**—The process of associating each bit transmitted by a service into the SONET payload structure that carries the service. E.g., mapping a DS1 service into a SONET VT1.5 associates each bit of the DS1 with a location in the VT1.5.

**Message Handling System (MHS)**—The system of message user agents, message transfer agents, message stores, and access units which together provide OSI electronic mail. MHS is specified in the CCITT X.400 series of recommendations.

**Multi-partite Virus**—A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector and parasitic viruses.

**Native Application**—Term given to an application that is written to use any communications protocol prior to ATM.

**Network**—A collection of computers and other devices that are able to communicate with each other over some network medium.

**Network Address**—(1) Also called a protocol address. A network layer address referring to a logical, rather than a physical, network device. (2) Numeric character string used to specify the location of the called customer.

**Network Analyser**—A hardware/software device offering various network troubleshooting features, including protocol-specific packet decodes, specific pre-programmed troubleshooting tests, packet filtering, and packet transmission.

**Network Byte Order**—The Internet-standard ordering of the bytes corresponding to numeric values.

**Network Driver Interface Specification (NDIS)**—Produced by Microsoft, a specification for a generic, hardware-independent and protocol-independent device driver for NICs.

**Network-Level Firewall**—A firewall in which traffic is examined at the network protocol packet level.

**Network File System (NFS)**—A distributed file system developed by Sun Microsystems which allows a set of computers to cooperatively access each other's files in a transparent manner.

**Network Layer**—Layer 3 of the OSI reference model. Layer 3 is the layer at which routing occurs.

**Network Management System (NMS)**—A system responsible for managing at least part of a network. NMSs communicate with agents to help keep track of network statistics and resources.

**Network Number**—The part of an Internet address that specifies the network to which the host belongs.

**Node**—One of a number of UNIX Computers joined together to form a Staffware Network.

**Open Data-link Interface (ODI)**—Novell specification for a multi-protocol API allowing NetWare and other transport protocols to share a common network interface card for PCs on a LAN.

**Packet**—(1) A logical grouping of information that includes a header and (usually) user data. (2) Continuous sequence of binary digits of information is switched through the network and an integral unit. Consists of up to 1024 bits (128 octets) of customer data plus additional transmission and error control information.

**Packet Buffer**—Storage area to hold incoming data until the receiving device can process the data.

**Packet Filtering**—A second layer of filtering on top of the standard filtering provided by a traditional transparent bridge. Can improve network performance, provide additional security, or logically segment a network to support virtual workgroups.

**Packet Switch**—The vehicle of the Local Public Data Network which performs the switching function. For Local Public Data Network service, this is a Telephone Company facility Hub.

**Packet Switching**—(1) Type of data transfer that occupies a communication link only during the time of actual data transmission. Messages are split into packets and reassembled at the receiving end of the communication link. (2) A transmission technique that segments and routes information into discrete units. Packet switching allows for efficient sharing of network resources as packets from different sources can all be sent over the same channel in the same bitstream.

**Parasitic Virus**—A computer virus which attaches itself to another computer program, and is activated when that program is executed.

**Parity Check**—An error checking scheme which examines the number of transmitted bits in a block which hold the value one. For even parity, an overhead parity bit is set to either one or zero to make the total number of transmitted ones in the block data plus parity bit an even number. For odd parity, the parity bit is set to make the total number of ones in the block an odd number.

**Password**—A group of characters assigned to a staffware user by the system administrator and used to sign off some forms.

**Password Authentication Protocol (PAP)**—A simple password protocol that transmits a user name and password across the network, unencrypted.



**Payload**—(1) That portion of a frame or cell that carries user traffic, that is, the frame or cell exclusive of any headers or trailers. (2) The service carried by a SONET carrier; the contents of an STS SPE or VT SPE.

**Payload Type Indicator (PTI)**—A three-bit field contained in the ATM cell header. The first bit indicates which AAL to be used to format the data in the payload; the second provides Explicit Forward Congestion Indication (EFCI); the third indicates whether the cell contains data Operations, Administration, and Maintenance (OAM) information.

**Perimeter-Based Security**—The technique of securing a network by controlling access to all entry and exit points of the network.

**Perimeter Firewall**—There are two types of perimeter firewalls: static packet filtering and dynamic firewalls. Both work at the IP address level, selectively passing or blocking data packets. Static packet filters are less flexible than dynamic firewalls.

**Piggybacking**—The inclusion of an acknowledgment of a previously received protocol data unit in an outgoing protocol data unit.

**Polymorphic Virus**—Self-modifying encrypting virus.

**Protocol**—(1) A formal description of a set of rules and conventions that govern how devices on a network exchange information. (2) Set of rules conducting interactions between two or more parties. These rules consist of syntax (header structure) semantics (actions and reactions that are supposed to occur) and timing (relative ordering and direction of states and events). (3) A formal set of rules.

**Proxy**—The mechanism whereby one system “fronts for” another system in responding to protocol requests.

Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

**Remote Access**—The process of allowing remote workers to access a corporate LAN over analog or digital telephone lines.

**Remote Access Server**—Access equipment at a central site that connects remote users with corporate LAN resources.

**Remote Bridge**—A bridge that connects physically disparate network segments via WAN links.

**Remote File System (RFS)**—A distributed file system, similar to NFS, developed by AT&T and distributed with their UNIX System V operating system.

**Remote Monitoring (RMON)**—Subset of SNMP MIB II allows flexible and comprehensible monitoring and management capabilities by addressing up to ten different groups of information.

**Remote Network**—The access equipment and telephone lines that connect remote users at multiple locations to the corporate LAN.

**Remote Operations Service Element (ROSE)**—The OSI RPC mechanism used in OSI Message Handling, Directory, and Network Management application protocols.

**Resolution**—The amount of detail that can be seen in an image. The resolution of a TV screen is defined in terms of the number of horizontal lines of picture elements that the screen displays.

**Restricted Access**—A security measure which admits or rejects callers by checking them against a list of remote node addresses programmed into a central site server.

**Ring Topology**—Topology in which the network consists of a series of repeaters connected to one another by unidirectional transmission links to form a single closed loop. Each station on the network connects to the network at a repeater.

**Router**—An OSI Layer 3 device that can decide which of several paths network traffic will follow based on some optimality metric. Also called a gateway (although this definition of gateway is becoming increasingly outdated), routers forward packets from one network to another based on network-layer information.

**Security**—Protection against unwanted behavior. The most widely used definition of (computer) security is secure = confidentiality + integrity + availability.

**Security Policy**—A security policy is the set of rules, principles, and practices that determine how security is implemented in an organization. It must maintain the principles of the organization's general security policy.

**Scrambling**—Coding the output of a SONET transmitter to assure adequate density for the receiving end to detect the signal. SONET scrambling compares the current transmitted bit to several previously transmitted bits and changes its value based on the result of that comparison. The receiving end decodes the scrambling.

**Shared Network Arrangement**—A service offering whereby a service user may connect subtending services to a host subscriber's multiplexed high capacity service. The telephone company will then undertake to maintain separate customer records and billing.

**Simple Mail Transfer Protocol (SMTP)**—Protocol governing mail transmissions. It is defined in RFC 821, with associated message format descriptions in RFC 822.

**Simple Network Management Protocol (SNMP)**—The Internet network management protocol. SNMP provides a means to monitor and set network configuration and runtime parameters.

**Small Computer Serial Interface (SCSI)**—Physical interface standard between high speed external devices, such as disks and CD-ROMs, and desktop systems.

**Spoofing**—A method of fooling access equipment into thinking a network connection is active even when it's not.

**Star Topology**—A topology where devices are connected to a central point such as a hub.

**Stealth Virus**—A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.

**SubNetwork Protocol (SNP)**—(TCP/IP) Protocol residing in the SubNetwork layer below IP that provides data transfer through the local subnet. In some systems, an adapter module must be inserted between IP and the SubNetwork Protocol to reconcile their dissimilar interfaces.

**Synchronous Payload Envelope (SPE)**—A SONET structure that carries the payload (service) in a SONET frame or virtual tributary. The STS SPE may begin anywhere in the frame's payload envelope. The VT SPE may begin anywhere in a floating mode VT but begins at a fixed location in a locked mode VT.

**System Administrator**—The person responsible for maintaining Staffware data not specific to individual procedures, such as user data.

**Systems Applications Architecture (SAA)**—SNA plan to allow programs on different computers to communicate.

Systems Network Architecture (SNA)—IBM's proprietary network architecture.

T1—Digital transmission facility operating with a nominal bandwidth of 1.544 Mbps. Also known as Digital Signal Level 1 (D1). Composed of 24 DS-0 channels in many cases. The T1 digital transmission system is the primary digital communication system in North America.

T3—Digital transmission facility operating at 45 Mbps bandwidth. Composed of 28 DS-1 channels in many cases. Also known as DS-3.

Token Ring—As defined in IEEE 802.5, a communications method that uses a token to control access to the LAN. The difference between a token bus and a token ring is that with a token ring, LAN does not use a master controller to control the token. Instead, each computer knows the address of the computer that should receive the token next. When a computer with the token has nothing to transmit, it passes the token to the next computer in line.

Traffic Shaping—Allows the sending station to specify the priority and throughput of information going into the ATM network and subsequently monitor information progress to meet required service levels.

Trivial File Transfer Protocol (TFTP)—A simplified version of FTP allowing the transfer of files from one computer to another over a network.

Trojan Horse—(1) A software entity that appears to do something normal but which, in fact, contains a trapdoor or attack program. (2) A computer program whose execution would result in undesired side effects, generally unanticipated by the user. The trojan horse program may otherwise give the appearance of providing normal functionality.

Unauthorized Switching—Long distance services that are switched to a new long distance company

without consumers permission. Such unauthorized switching violates FCC rules and consumer protection policies.

Unicast Address—An address specifying a single network device.

Unified Network Management Architecture (UNMA)—AT&T's umbrella software system.

Uploading—Sending a text file or software program via telecommunications to another computer. See Downloading.

Username—This is the name assigned to you for Staffware login. (It is the same as your UNIX login name.)

Validation List—A dropdown list of values attached to a field from which you select one.

Value Added Network (VAN)—A national (or international) enhanced network that is designed expressly to carry data communications. VANs also provide billing and other special services to their customers.

Versatile Message Transport Protocol (VMTP)—Designed at Stanford to replace TCP and TP4 in high-speed networks.

Vertical Integration—The involvement of cable systems in other links in the video distribution chain, such as program production and supply.

Virtual IP—A function provided on the Catalyst with the Virtual Network Services software which enables the creation of logically separated switched IP workgroups across Catalyst switch ports.

Virtual LAN—Membership to a Virtual LAN is defined administratively independent of the physical network topology. A virtual LAN segment is a unique broadcast domain.

**Virus**—A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

**Virus Signature**—An identifier recognized by the virus as meaning “this item is already infected, do not reinfect.” It can take different forms such as the text “sURIV” at the beginning of the file, the size of the file divisible by a number or the number of seconds in the date stamp set to 62. Some viruses do not recognize their signatures correctly.

**Wide Area Information Servers (WAIS)**—WAIS allows users to search and access different types of information from a single interface. The WAIS protocol is an extension of the ANSI Z39.50 information retrieval protocol.

**Wide Area Network (WAN)**—(1) A network which encompasses interconnectivity between devices over a wide geographic area. Such networks would require public rights-of-way and operate over long distances. (2) A set of computers that communicate with each other over long distances.

**Workgroup**—A group of workstations and servers that commonly exchange data. This term is also used to describe a group of people who work together.

**Workgroup Switching**—The ability to handle asymmetric traffic patterns via high-speed (100 Mbps) interface and intelligent switching.

**Workstation (WS)**—A terminal or computer that provides craft access to a network element.

NOTES

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

NOTES

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

# Cheyenne Security Center

The most comprehensive on-line resource for computer security and virus information.

- The Latest Info on Security Products
- Hot Security News
- On-line Monthly Newsletter
- Interactive Ask the AntiVirus Experts Forum
- First On-line Virus Clinic
- Virus Encyclopedia, and more...

**Visit us today!**

Visit ATG's Web Site  
to read, download, and print  
all the Technology Guides  
in this series.

<http://www.techguide.com>

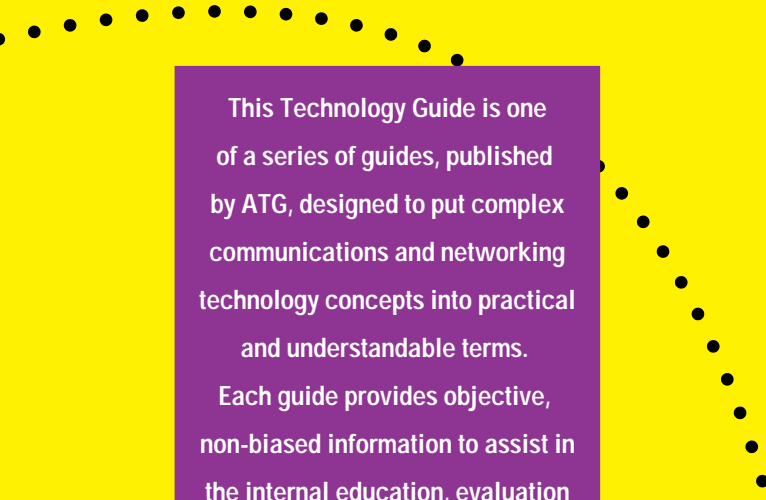


“The significant problems we face cannot be solved by the same level of thinking that created them.”

Albert Einstein

**CHEYENNE**<sup>®</sup>  
A Division of Computer Associates

[www.cheyenne.com/security](http://www.cheyenne.com/security)

A decorative dotted line of black dots curves across the top and right side of the page.

This Technology Guide is one of a series of guides, published by ATG, designed to put complex communications and networking technology concepts into practical and understandable terms.

Each guide provides objective, non-biased information to assist in the internal education, evaluation and decision making process.

This Technology Guide, as well as the other communications and networking technology guides in the series, are available on ATG's Web Site.

<http://www.techguide.com>

Produced and Published by



One Apple Hill, Suite 216, Natick, MA 01760

Tel: (508) 651-1155 Fax: (508) 651-1171 E-mail: [info@techguide.com](mailto:info@techguide.com)