Security on IP Networks

Countering Denial of Service (DoS) Attacks

An Overview of the Key Challenges and Countermeasures

Over the past few years, as networks have become ubiquitous and intricately intertwined, security issues have pushed to the forefront of concern for everyone involved, including end users, administrators, and equipment suppliers. Despite the collaborative efforts that have brought about improved network security measures, the covert actions of hackers and cyber-terrorists continue to pose a serious threat.

For example, in 1998, hackers were able to penetrate government computers and gain “root” access – meaning they had the capability to shut the systems down, steal or alter confidential information. In 1999, the Melissa macro virus caused at least $80 million in damage and affected networks and systems worldwide.

In 2000, denial-of-service (DoS) attacks have emerged as the latest threat to globally linked networks. In just the few months since their first appearance, DoS attacks have already taken some of the most popular e-commerce sites off-line for several hours, causing enormous losses and repair costs.
# Table of Contents

## Introduction
- The Rising Challenges from Denial-of-Service (DoS) Attacks
  - Modes of Attack
  - Trends in DoS Attacks
  - Specific Types of DoS Attacks
  - SYN-ACK Attacks or TCP-SYN Flooding
  - Teardrop Attacks
  - Smurf Attacks
  - Oversized Packet Attacks
  - UDP Flood Attacks
  - Adverse Impacts of DoS Attacks

## Implementing Countermeasures Against DoS Attacks
- LAN Level Issues
- Network Transport Level Issues

## Protecting Network Dataflow
- Wire-speed Layer-independent QoS and Access Control Options
- Customizable Filtering and "Trusted Neighbor" Mechanisms
- Tailored Network Login Provisions

## Protecting the Network Infrastructure
- System Management Disciplines

## Controlling Access
- Management Access
- User Account
- Administrator Account
- Telnet
- SSH2
- Simple Network Management Protocol (SNMP) Access
- Authenticating Access
  - RADIUS
  - TACACS+
  - Differences Between RADIUS and TACACS+

## Access Policies
- Access Lists
- Routing Access Policies
- Route Maps

## Forwarding-controls and Load-balancing Methods

## Rigorous DoS Stress Testing

## The Bottom Line

The Rising Challenges from Denial-of-Service (DoS) Attacks

DoS attacks are typically aimed at services connected to the Internet with the intent of degrading or disabling the service so that the services become unavailable to legitimate users. This is usually attempted by flooding the target system with the intent of overloading the system with additional traffic. DoS attacks focus on overloading the system with both legitimate and malicious traffic so that legitimate traffic can be blocked or otherwise degraded.

Types of Attacks

DoS attacks come in a variety of forms and sizes at a variety of service providers. There are three basic types of attacks:

- Consumption of seized, limited or non-renewable resources
- Destruction of available or configuration information
- Physical destruction or destruction of network components

Specific DoS attacks can be executed using limited resources against a large, sophisticated web site or network. Some DoS attacks can be executed with limited resources against a large, sophisticated web site or network.

- Attacks to flood the target systems to access confidential data
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to "flood" a network, thereby preventing legitimate traffic

Typical examples of recent trends in DoS attacks have included:

- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to "flood" a network, thereby preventing legitimate traffic

Some DoS attacks can be executed using limited resources against a large, sophisticated web site or network. Some DoS attacks can be executed with limited resources against a large, sophisticated web site or network.

Traffic Flowing-through Attack

A SYN-ACK attack exploits the TCP/IP mechanism by using a three-way handshake in order to establish a connection. SYN-ACK attacks force the server to store huge numbers of acknowledgement packets in its backlog queue, with the objective of overflowing the queue and disabling the server’s ability to issue acknowledgements. When there are multiple match statements in an entry, the entry is considered a successful match.

Traffic Flowing-through Attack

A SYN-ACK attack forces the server to store huge numbers of acknowledgement packets in its backlog queue, with the objective of overflowing the queue and disabling the server’s ability to issue acknowledgements. When there are multiple match statements in an entry, the entry is considered a successful match.

Traffic Flowing-through Attack

A SYN-ACK attack forces the server to store huge numbers of acknowledgement packets in its backlog queue, with the objective of overflowing the queue and disabling the server’s ability to issue acknowledgements. When there are multiple match statements in an entry, the entry is considered a successful match.

Traffic Flowing-through Attack

A SYN-ACK attack forces the server to store huge numbers of acknowledgement packets in its backlog queue, with the objective of overflowing the queue and disabling the server’s ability to issue acknowledgements. When there are multiple match statements in an entry, the entry is considered a successful match.

Forwarding-controls and Load-balancing Methods

Because some DoS attacks result from intruders understanding your routing policies, it is also important to maintain tight control over basic policy disciplines such as IP-ESP and IP-MS. Load-balancing methods can be tailored to provide end-to-end simplicity and maximum resiliency by incorporating critical features such as end-to-end simplicity and maximum resiliency. Forwarding controls can be tailored to provide end-to-end simplicity and maximum resiliency. Load-balancing methods can be tailored to provide end-to-end simplicity and maximum resiliency.

Rigorous DoS Stress Testing

The final area of critical importance is ensuring that the switching and routing systems themselves undergo rigorous design tests to ensure reliability and robustness, even when directly subjected to the most challenging DoS stress testing. Achieving these objectives depends on the robustness of the system architecture and is ultimately tested using real-world DoS attacks.

All Extreme switches and the ExtremeWare software suite share the same consistent architecture to provide end-to-end simplicity and maximum reliability by incorporating critical features such as end-to-end simplicity and maximum reliability. Load-balancing methods can be tailored to provide end-to-end simplicity and maximum reliability.

Summary

The Extreme Networks solution allows service providers to keep it simple and keep it fast. Extreme provides a network infrastructure that combines guaranteed latency and reliability with the unmatched data capacity, scalability and low cost of an Ethernet network. Extreme’s switches offer simplified traffic management and traffic engineering that guarantee service level commitments. Each Extreme switch supports the range of network management and traffic engineering that guarantee service level commitments, while service providers can control priorities by classifying and remarking packets as they enter the network.

Traffic Management does not have to be Complicated

Service providers need solutions that enable them to deliver high-value services to their subscribers and to preserve these new services quickly, with minimal administrative overhead. With Extreme’s policy management system service providers can easily reach these goals.

While traffic management can involve an intricate array of technologies, business, and products, Extreme simplifies the issue by building traffic management capability into every Extreme switch. This simplifies network design and reduces costs. Because of Extreme’s basic-based implementation, traffic management always runs at wire-speed for all ports with no performance impact, even when additional switch functions such as server load balancing are enabled.

In addition, service providers can provision bandwidth for each subscriber by defining policies that specify minimum and maximum bandwidths. This effectively allocates a "pipe" to each subscriber, assuring that each subscriber gets the correct amount of bandwidth while ensuring bandwidth is available to other users.

Traffic can be prioritized within each pipe by either the subscriber or the service provider. Subscribers can use policies to maintain queues at the appropriate DiffServ code point before the packets enter the service provider network, while service providers can control priorities by classifying and remarking packets as they enter the network.

Traffic Management does not have to be Complicated

Service providers need solutions that enable them to deliver high-value services to their subscribers and to preserve these new services quickly, with minimal administrative overhead. With Extreme’s policy management system service providers can easily reach these goals.

While traffic management can involve an intricate array of technologies, business, and products, Extreme simplifies the issue by building traffic management capability into every Extreme switch. This simplifies network design and reduces costs. Because of Extreme’s basic-based implementation, traffic management always runs at wire-speed for all ports with no performance impact, even when additional switch functions such as server load balancing are enabled.

In addition, service providers can provision bandwidth for each subscriber by defining policies that specify minimum and maximum bandwidths. This effectively allocates a "pipe" to each subscriber, assuring that each subscriber gets the correct amount of bandwidth while ensuring bandwidth is available to other users.

Traffic can be prioritized within each pipe by either the subscriber or the service provider. Subscribers can use policies to maintain queues at the appropriate DiffServ code point before the packets enter the service provider network, while service providers can control priorities by classifying and remarking packets as they enter the network.

Traffic Management does not have to be Complicated

Service providers need solutions that enable them to deliver high-value services to their subscribers and to preserve these new services quickly, with minimal administrative overhead. With Extreme’s policy management system service providers can easily reach these goals.

While traffic management can involve an intricate array of technologies, business, and products, Extreme simplifies the issue by building traffic management capability into every Extreme switch. This simplifies network design and reduces costs. Because of Extreme’s basic-based implementation, traffic management always runs at wire-speed for all ports with no performance impact, even when additional switch functions such as server load balancing are enabled.

In addition, service providers can provision bandwidth for each subscriber by defining policies that specify minimum and maximum bandwidths. This effectively allocates a "pipe" to each subscriber, assuring that each subscriber gets the correct amount of bandwidth while ensuring bandwidth is available to other users.

Traffic can be prioritized within each pipe by either the subscriber or the service provider. Subscribers can use policies to maintain queues at the appropriate DiffServ code point before the packets enter the service provider network, while service providers can control priorities by classifying and remarking packets as they enter the network.
Access Lists

IP access lists consist of IP access rules that are used to permit or deny packets in an incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order. Then, it is either forwarded to a specified QoS profile or dropped. Using access lists has no impact on switch performance. Access lists are typically applied to traffic that cross Layer 3 routed boundaries, but it is also possible to use access lists within a Layer 2 VLAN.

Each entry that makes up an IP access list contains a unique name. It can also contain an optional, unique procedure data. The rules of an IP access list consist of a combination of the following six components:
- IP source address and mask
- IP destination address and mask
- TCP or UDP source port range
- TCP or UDP destination port range
- A physical source port
- A precedence number (optional)

When a packet arrives on an ingress port, the packet is compared with the access list rules to determine a match. When a match is found, the packet is processed. If the access list is of type deny, the packet is dropped. If the list is of type permit, the packet is forwarded. A permit access list can also apply a QoS profile to the packet.

Routing Access Policies

Routing access policy controls the advertisement or rejection of routing protocols such as RIP, OSPF or BGP. Routing access policies can be used to “hide” entire networks or to trust only specific sources for routes or ranges of routes. The capabilities of routing access policies are specific to the type of routing protocol involved. However, they are sometimes more efficient and easier to implement than access lists.

Route Maps

Route maps can be used to control the redistribution of routes between two routing domains and to modify the routing information that is redistributed. Route maps are used in conjunction with the match and set operations. A match operation specifies a criteria that must be matched. A set operation specifies a change that is made to the route when the match operation has succeeded. Route maps are used to modify or filter routes redistributed into BGP. They are also used to modify or filter the routing information exchanged with BGP neighbors.

Teardrop Attacks

Teardrop attacks exploit IP mechanisms involved in the reassembly of packets that have been disassembled for efficient transmission. In normal practice, each packet fragment looks like the original IP packet with the exception of an offset field that specifies which bytes of the original packet are included (i.e., bytes 400 through 4000), thereby enabling the receiving system to reassemble all of the data in the proper sequence. By purposely creating packet fragments with overlapping offset fields, these types of attacks make it impossible for the victim’s system to correctly reassemble the packet fragments, which can sometimes cause the victim system to hang, crash, or reboot.

Smart Attacks

Smart attacks take advantage of doS attack mechanisms by spoofing the target system’s IP address and broadcasting Internet Control Message Protocol (ICMP) ping requests across multiple subnets. This attack cloaks the victim’s network with bogus ICMP echo requests and responses, thereby making it unavailable to legitimate traffic. All intermediary systems that are co-opted or drawn into the echo-response cycle become victims of this attack, both suffering from and contributing to overall network congestion.

Oversized Packet Attacks

Oversized packet attacks exploit a known bug in some TCP/IP implementations by using the ping utility to send packets that exceed the maximum 65,536 bytes of data allowed by the IP specification. When it first emerged, this type of attack caused crashes, hangs or reboots in victim’s systems. However, most operating system vendors have now addressed this issue with software updates that enable smooth disposition of oversized packets.

UDP Flood Attacks

UDP Flood attacks exploit User Datagram Protocol (UDP) mechanisms by creating bogus UDP connections between unsuspecting systems. When a connection is established between two UDP services, each of which produces output, the combined effects can produce a very high number of packets and result in denial of service to legitimate users. In UDP flood attacks, the intruders use forged UDP packets to connect the echo service on one machine to the chargen service on the other machine, causing the two machines to consume all available bandwidth on the connection between them.
Adverse Impacts of DoS Attacks

Using relatively simple assault methods, DoS attacks can completely disable target systems or even disrupt entire networks by not allowing them to function properly. A DoS attack can bring entire organizations to a complete standstill, thereby costing millions of dollars in lost revenue and/or productivity.

For example, some recent high-profile DoS attacks have targeted major Internet portals or e-commerce sites by disabling web site access for extended periods of time and resulting in loss of revenue and credibility. In other cases, DoS attacks have been aimed at disrupting and disabling major Internet service providers (ISPs), causing widespread havoc among all users across large geographic areas.

Implementing Countermeasures Against DoS Attacks

Effective protection against DoS attacks involves taking countermeasures at all levels across the internetworking infrastructure, including taking specific actions at the LAN level and addressing broader issues at the network transport level.

LAN Level Issues

At the LAN level, system administrators can take a number of preventive measures to guard against the disabling effects of DoS attacks. These preventive measures range from maintaining solid overall administrative and security procedures to implementing specific safeguards targeted at countering each of the various types of DoS attacks.

For example, while it is virtually impossible to completely eliminate spoofing of IP packets, system administrators can effectively reduce the risk of internally fueled spoofed IP attacks by instituting filtering actions that restrict the flow of data input if they have source addresses from within the internal network. In addition, administrators can reduce the risk of being used as an intermediary in spoofed IP DoS attacks by installing filters to restrict the external flow of IP packets with source addresses that don’t originate within the internal network.

Other methods associated with specific types of DoS attacks may include turning off or restricting specific services that might otherwise be compromised or subverted. For instance, UDP services could be restricted for use only within the internal network, thus keeping UDP available for network diagnostic purposes only. This prevents its unauthorized use for UDP flooding attacks.

Unfortunately, such restrictive measures must also be weighed against the impact they may have on legitimate applications, such as RealAudio that uses UDP as the transport mechanism. If attackers are able to intimidate victims into not using beneficial IP services or legitimate applications, to some extent, they have accomplished their objectives.

Distribution of Functionality

The RADIUS protocol combines the processes of authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication and authorization functions difficult. The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, as seen in many service provider networks.

During a session, if additional authorization checking is required, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This feature provides greater control over the commands that can be executed on the access server while decoupling authorization from the authentication mechanism. TACACS+ is thus more appropriate to use when multiple authentication methods in a complex network are deployed.

Multiprotocol Support

RADIUS has limited support for protocols other than TCP/IP. For example, RADIUS does not natively support the following protocols:

- AppleTalk Remote Access (ARA)
- NetBIOS frame protocol control
- Novell Asynchronous Services Interface (NASI)
- Packet Assembler/Disassembler (PAD) connection

These protocols are natively supported by TACACS+.

Access Policies

Once access to the network is authenticated, the next step is to protect networked resources. These resources or nodes are where intellectual property and confidential information reside. Access policies are a general category of preset decision making rules that impact forwarding and route forwarding decisions. Access policies are used primarily for security and QoS purposes. There are three categories of access policies: access lists, routing access policies and route maps.
In addition to authenticating users, the Extreme TACACS+ implementation delivers the mechanism to perform authorization and accounting similar to RADIUS.

**Differences between RADIUS and TACACS+**

Although these two protocols provide similar functionality, they have several key differences.

**Transport Mechanism**

The most fundamental difference between TACACS+ and RADIUS is the network transport protocol that each one uses. The RADIUS protocol uses UDP to exchange information between the NAS and the access control server, whereas TACACS+ uses the Transmission Control Protocol (TCP). TCP is a connection-oriented transport protocol, whereas UDP offers best-effort delivery. RADIUS utilizes additional, programmable variables to control factors such as retransmit attempts and timeouts in order to compensate for the best-effort transport provided by UDP. TACACS+ does not need these extra variables because connection issues are handled transparently by the TCP protocol.

TCP provides a separate acknowledgment via a TCP acknowledgment packet when a request has been received by the access control server within an acceptable network round-trip time. This acknowledgment occurs regardless of the congestion of the access control server.

TCP provides immediate indication of an unavailable server. Long-lived TCP connections will even reveal servers that go down and then come back up. UDP is unable to discriminate between a down server, a slow server and a non-existent server.

Using TCP keep-alives, server crashes can be detected out of band with actual requests. Connections to multiple servers can be maintained simultaneously and messages need to be sent only to servers that are known to be up and running. TCP provides a stable foundation that is scalable for all types of networks.

**Confidentiality**

RADIUS encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is in the clear. Other information such as username, authorized services and accounting can be captured by a third party, making RADIUS networks potential targets of hackers using session capture and replay attacks. Because of this feature, RADIUS networks must be carefully designed to minimize DoS attacks.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether or not the body is encrypted. Normal operation fully encrypts the body of the packet for more secure communications.

**Network Transport Level Issues**

While actions taken by LAN administrators are key to laying the groundwork for preventing and combating DoS attacks, they must also be supplemented by comprehensive countermeasures instituted at the network transport level. These network transport issues fall into two categories:

- Actively policing internetwork level dataflows to identify DoS attacks and protect users and subnets against their impacts
- Protecting the internetworking infrastructure’s switching and routing equipment to ensure resiliency against DoS attacks

**Protecting Network Dataflow**

Effectively protecting network dataflow involves a variety of complementary strategies, including using multilayer switching for layer-independent access control, leveraging customizable filtering and “trusted neighbor” criteria, and controlling network login access by unauthorized users.

**Wire-speed Layer-independent Quality of Service (QoS) and Access Control Options**

The emergence of wire-speed multilayer switching systems with intelligent software-configurable, layer-independent QoS and access control capabilities are significantly improving the ability of network transport infrastructures to protect dataflow integrity.

With conventional router-based network infrastructures, authentication mechanisms such as filtering out spoofed packets with internal addresses would require traffic to hit the router boundary and be matched against criteria in specific access control lists. Maintaining access control lists makes this procedure very time consuming, while imposing significant overhead on overall router performance.

In contrast, the use of wire-speed multilayer switching allows the flexible implementation of a variety of policy-based access control criteria, using many of the same mechanisms that have become vital for effectively implementing QoS criteria throughout complex network infrastructures.

Prior to granting network authorization, the network administrator must use certain protocols to perform the authentication. In today's networks, TACACS+ and RADIUS protocols are commonly used to provide robust security.

**RADIUS**

The RADIUS protocol was developed as an access server authentication and accounting protocol. RADIUS (IETF RFC 2138) is a mechanism for authenticating and centrally administrating access to network nodes. The ExtremeWare RADIUS client implementation allows authentication for telnet, HTTP or console access to all Extreme switches.

First, a primary and secondary RADIUS server is defined for the switch to contact. When a user attempts to login, the request is sent to the primary RADIUS server and then to the secondary server, if the primary does not respond. If the RADIUS client is enabled but access to the primary and secondary server fails, Extreme switches will use its local database for authentication. The privileges assigned to the user (admin vs. non-admin) at the RADIUS server take precedence over the configuration in the local switch database.

The ExtremeWare RADIUS implementation also supports per-command authentication. Per-command authentication allows the definition of several levels of user authorization by controlling the permitted command sets based on RADIUS usernames and passwords. This is made possible using the Extreme-modified RADIUS Merit software. The Merit AAA server application is the most commonly used and most publicly available implementation of RADIUS servers. The software is available in compiled format for Solaris™ or Linux™, as well as in source code format.

**TACACS+**

Privileged and non-privileged mode passwords are global and apply to every user accessing a switch from either the console port or from a telnet session. As an alternative, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network. TACACS+ was derived from the U.S. Department of Defense and is described in IETF RFC 1492.

The ExtremeWare version of TACACS+ can be used to authenticate users who are attempting to administer the switch. The TACACS+ protocol is used to communicate between the switch and an authentication database. With TACACS+ enabled, Extreme switches will prompt the user for a username and password. Then, the switch queries the TACACS+ server to verify the supplied information. The TACACS+ server typically runs on a UNIX workstation and quite a few implementations are available in the public domain.
The ExtremeWare™ software suite from Extreme Networks® allows mapping and overwriting of IEEE 802.1p and DiffServ tags to enable DiffServ functionalities that are invisible to external observation. By using these policy mechanisms, system administrators can adjust internal routing control policies for traffic from specific neighboring systems without advertising the actual policies being internally enforced.

Secure Shell 2 (SSH2)
FIPS-186 (Federal Information Processing Standards Publication 186) SSH2 is a feature of ExtremeWare that encrypts telnet session data between the switch and a network engineer using SSH2 client software. The ExtremeWare SSH2 switch application is based on the DataFellows™ SSH2 server implementation. This requires F-Secure® SSH client products from DataFellows Corporation on the network engineer’s workstation.

Because SSH2 is currently under U.S. export restrictions, before enabling SSH2, you must first obtain a security license (at no extra charge) from Extreme. Go to the Extreme web site at www.extremenetworks.com/go/security.htm and fill out the contact form to indicate compliance or non-compliance with export restrictions. When in compliance, information will be made available to enable the security features.

An authentication key must be generated for each SSH2 session. This can be done automatically by Extreme switches or by the client application. The supported cipher is 3DES-CBC (IETF RFC 1851). The supported key exchange is DSA (IETF RFC 2792).

Simple Network Management Protocol (SNMP) Access
Any network administrator running SNMP can manage Extreme switches if the Management Information Base (MIB) is installed correctly on the management station. Non-privileged access (SNMP read access) allows users on a host to send the switch SNMP get-request and SNMP get-next-request messages. These messages are used to gather information and statistics from the switch. Privileged access (SNMP read/write access) allows users on a host to send the switch SNMP set-request messages in order to make changes to the switch’s configurations and operational settings.

SNMP access allows you to set up different SNMP community strings for both non-privileged and privileged access. The default read-access community string on Extreme switches is public, while the default read/write access community string on Extreme switches is private.

An authentication key must be generated for each SSH2 session. This can be done automatically by Extreme switches or by the client application. The supported cipher is 3DES-CBC (IETF RFC 1851). The supported key exchange is DSA (IETF RFC 2792).

Simple Network Management Protocol (SNMP) Access
Any network administrator running SNMP can manage Extreme switches if the Management Information Base (MIB) is installed correctly on the management station. Non-privileged access (SNMP read access) allows users on a host to send the switch SNMP get-request and SNMP get-next-request messages. These messages are used to gather information and statistics from the switch. Privileged access (SNMP read/write access) allows users on a host to send the switch SNMP set-request messages in order to make changes to the switch’s configurations and operational settings.

SNMP access allows you to set up different SNMP community strings for both non-privileged and privileged access. The default read-access community string on Extreme switches is public, while the default read/write access community string on Extreme switches is private.

For more information on DataFellows’ SSH2 server implementation, visit their web site at www.datafellows.com.

Tailoring routing access policies can ensure “trusted neighbor” relationships to prevent unauthorized access to networks.

The ExtremeWare™ software suite from Extreme Networks® allows mapping and overwriting of IEEE 802.1p and DiffServ tags to enable DiffServ functionalities that are invisible to external observation. By using these policy mechanisms, system administrators can adjust internal routing control policies for traffic from specific neighboring systems without advertising the actual policies being internally enforced.

The flexibility to differentiate between internal and external DiffServ and IEEE 802.1p criteria can be an effective tool for thwarting a new wave of potential DoS attacks referred to as QoS attacks. In the instances that have appeared so far, these attacks attempt to make use of bogus QoS criteria in order to adversely impact network routing behaviors. It does this by spoofing high-priority traffic classifications and usurping bandwidth away from legitimate QoS classes.

ExtremeWare’s ability to maintain invisible internal DiffServ handling policies enables all Extreme switches to easily ignore, observe or manipulate any DiffServ tags received from a potentially "untrusted neighbor."

Tailored Network Login Provisions
The incorporation of network login mechanisms play a key role in reducing vulnerability to DoS attacks.

Network login works by using unique usernames and passwords to authenticate users before granting access or passing packet traffic, thereby preventing the risk of pre-authentication DoS assaults.

By using DHCP to emulate how the dial-up world uses PPP, network login can stop unauthorized access at the edge of the network and mitigate any negative impact on the network infrastructure. Network login works by having the user’s browser submit a DHCP request to the switch, which captures the required access information.

Any workstation with a telnet facility should be able to communicate with Extreme switches on the same network as the workstation. While the default setting on Extreme switches accepts telnet sessions, access can be restricted by using an access profile. An access profile accepts or denies a named list of IP addresses and subnet masks.

Secure Shell 2 (SSH2)
FIPS-186 (Federal Information Processing Standards Publication 186) SSH2 is a feature of ExtremeWare that encrypts telnet session data between the switch and a network engineer using SSH2 client software. The ExtremeWare SSH2 switch application is based on the DataFellows™ SSH2 server implementation. This requires F-Secure® SSH client products from DataFellows Corporation on the network engineer’s workstation.

Because SSH2 is currently under U.S. export restrictions, before enabling SSH2, you must first obtain a security license (at no extra charge) from Extreme. Go to the Extreme web site at www.extremenetworks.com/go/security.htm and fill out the contact form to indicate compliance or non-compliance with export restrictions. When in compliance, information will be made available to enable the security features.

An authentication key must be generated for each SSH2 session. This can be done automatically by Extreme switches or by the client application. The supported cipher is 3DES-CBC (IETF RFC 1851). The supported key exchange is DSA (IETF RFC 2792).

Simple Network Management Protocol (SNMP) Access
Any network administrator running SNMP can manage Extreme switches if the Management Information Base (MIB) is installed correctly on the management station. Non-privileged access (SNMP read access) allows users on a host to send the switch SNMP get-request and SNMP get-next-request messages. These messages are used to gather information and statistics from the switch. Privileged access (SNMP read/write access) allows users on a host to send the switch SNMP set-request messages in order to make changes to the switch’s configurations and operational settings.

SNMP access allows you to set up different SNMP community strings for both non-privileged and privileged access. The default read-access community string on Extreme switches is public, while the default read/write access community string on Extreme switches is private.

For more information on DataFellows’ SSH2 server implementation, visit their web site at www.datafellows.com.

Tailoring routing access policies can ensure “trusted neighbor” relationships to prevent unauthorized access to networks.

The ExtremeWare™ software suite from Extreme Networks® allows mapping and overwriting of IEEE 802.1p and DiffServ tags to enable DiffServ functionalities that are invisible to external observation. By using these policy mechanisms, system administrators can adjust internal routing control policies for traffic from specific neighboring systems without advertising the actual policies being internally enforced.

The flexibility to differentiate between internal and external DiffServ and IEEE 802.1p criteria can be an effective tool for thwarting a new wave of potential DoS attacks referred to as QoS attacks. In the instances that have appeared so far, these attacks attempt to make use of bogus QoS criteria in order to adversely impact network routing behaviors. It does this by spoofing high-priority traffic classifications and usurping bandwidth away from legitimate QoS classes.

ExtremeWare’s ability to maintain invisible internal DiffServ handling policies enables all Extreme switches to easily ignore, observe or manipulate any DiffServ tags received from a potentially "untrusted neighbor."

Tailored Network Login Provisions
The incorporation of network login mechanisms play a key role in reducing vulnerability to DoS attacks.

Network login works by using unique usernames and passwords to authenticate users before granting access or passing packet traffic, thereby preventing the risk of pre-authentication DoS assaults.

By using DHCP to emulate how the dial-up world uses PPP, network login can stop unauthorized access at the edge of the network and mitigate any negative impact on the network infrastructure. Network login works by having the user’s browser submit a DHCP request to the switch, which captures the required access information.
The ExtremeWare software suite implements both Terminal Access Controller Access Control System (TACACS+) and an extended version of the Remote Authentication Dial-In User Server (RADIUS). The RADIUS protocol (IETF RFC 2138) provides an efficient and secure mechanism for authenticating and centrally administering access to network nodes. The ExtremeWare RADIUS client allows authentication for telnet, HTTP and console access to all Extreme switches. As an alternative to privileged and non-privileged categories, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network.

The use of independent access lists based on source IP addresses can also help protect the remote management methodologies used to maintain, update and manage network switching and routing systems. ExtremeWare allows a different access profile to be used for each remote access method (web, SNMP read, SNMP read/write, telnet, SSH2). Additionally, specific services can be completely turned off when not required by the application scenarios.

The following sections provide more detailed information on how Extreme's broadband switching solutions can control access and implement access policies to prevent DoS attacks.

The ExtremeWare software suite implements both Terminal Access Controller Access Control System (TACACS+) and an extended version of the Remote Authentication Dial-In User Server (RADIUS). The RADIUS protocol (IETF RFC 2138) provides an efficient and secure mechanism for authenticating and centrally administering access to network nodes. The ExtremeWare RADIUS client allows authentication for telnet, HTTP and console access to all Extreme switches. As an alternative to privileged and non-privileged categories, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network.

The use of independent access lists based on source IP addresses can also help protect the remote management methodologies used to maintain, update and manage network switching and routing systems. ExtremeWare allows a different access profile to be used for each remote access method (web, SNMP read, SNMP read/write, telnet, SSH2). Additionally, specific services can be completely turned off when not required by the application scenarios.

The following sections provide more detailed information on how Extreme's broadband switching solutions can control access and implement access policies to prevent DoS attacks.

By leveraging existing standards within the constructs contained in IEEE draft 802.1, which members of Extreme Networks' technical team helped co-author, these network login mechanisms provide control over user access to the switch and minimize the risk of direct DoS attacks. At the same time, network login offers a robust mechanism for managing and tracking user connectivity and transactions within an enterprise or a service provider network.

**Network Login in Action**

By leveraging existing standards within the constructs contained in IEEE draft 802.1, which members of Extreme Networks’ technical team helped co-author, these network login mechanisms provide control over user access to the switch and minimize the risk of direct DoS attacks. At the same time, network login offers a robust mechanism for managing and tracking user connectivity and transactions within an enterprise or a service provider network.

**Protecting the Network Infrastructure**

In addition to protecting network dataflow, it is equally important to protect the network infrastructure from DoS attacks to ensure reliability and resiliency. Key to protecting the infrastructure are maintaining independent access lists, tightly managing forwarding-controls and load-balancing functions, and conducting rigorous design tests to ensure system resiliency.

**System Management Disciplines**

One of the first steps to enforce security is to ensure that users can only perform tasks they are authorized to do and obtain information that they are authorized to have, while preventing damage to data, applications and network systems. Since all of these enforcement actions are handled on systems that form the network, controlling access to these systems is extremely important.

Extreme’s broadband switches can be managed via console access, SNMP, HTTP or telnet using the ExtremeWare command line interface. For each remote access method, one can assign non-privileged access or privileged access for a user or group of users. Non-privileged access allows users to monitor the switch but not configure the switch. Privileged access allows the user to fully manage and configure the switch.

The ExtremeWare software suite implements both Terminal Access Controller Access Control System (TACACS+) and an extended version of the Remote Authentication Dial-In User Server (RADIUS). The RADIUS protocol (IETF RFC 2138) provides an efficient and secure mechanism for authenticating and centrally administering access to network nodes. The ExtremeWare RADIUS client allows authentication for telnet, HTTP and console access to all Extreme switches. As an alternative to privileged and non-privileged categories, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network.

The use of independent access lists based on source IP addresses can also help protect the remote management methodologies used to maintain, update and manage network switching and routing systems. ExtremeWare allows a different access profile to be used for each remote access method (web, SNMP read, SNMP read/write, telnet, SSH2). Additionally, specific services can be completely turned off when not required by the application scenarios.

The following sections provide more detailed information on how Extreme’s broadband switching solutions can control access and implement access policies to prevent DoS attacks.

**Controlling Access**

**Management Access**

ExtremeWare supports two levels of management accounts.

**User Account**

A user account allows viewing access to all manageable parameters with the exception of the user account database and SNMP community strings. A user account can also use the ping command to test device accessibility and change the password assigned to the specific account name. For this level of access, the ExtremeWare command line interface prompts end with a (>) sign.

**Administrator Account**

A administrator account allows viewing and changing of all manageable parameters. This account can add or delete users and change the password associated with any account name. For this level of access, the ExtremeWare command line interface prompts end with a (:) sign.
The ExtremeWare software suite implements both Terminal Access Controller Access Control System (TACACS+) and an extended version of the Remote Authentication Dial-In User Server (RADIUS). The RADIUS protocol (IETF RFC 2138) provides an efficient and secure mechanism for authenticating and centrally administering access to network nodes. The ExtremeWare RADIUS client allows authentication for telnet, HTTP and console access to all Extreme switches. As an alternative to privileged and non-privileged categories, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network.

The use of independent access lists based on source IP addresses can also help protect the remote management methodologies used to maintain, update and manage network switching and routing systems. ExtremeWare allows a different access profile to be used for each remote access method (web, SNMP read, SNMP read/write, telnet, SSH2). Additionally, specific services can be completely turned off when not required by the application scenarios.

The following sections provide more detailed information on how Extreme's broadband switching solutions can control access and implement access policies to prevent DoS attacks.

**Protecting the Network Infrastructure**

In addition to protecting network dataflow, it is equally important to protect the network infrastructure from DoS attacks to ensure reliability and resiliency. Key to protecting the infrastructure are maintaining independent access lists, tightly managing forwarding-controls and load-balancing functions, and conducting rigorous design tests to ensure system resiliency.

**System Management Disciplines**

One of the first steps to enforce security is to ensure that users can only perform tasks they are authorized to do and obtain information that they are authorized to have, while preventing damage to data, applications and network systems. Since all of these enforcement actions are handled on systems that form the network, controlling access to these systems is extremely important.

Extreme's broadband switches can be managed via console access, SNMP, HTTP or telnet using the ExtremeWare command line interface. For each remote access method, one can assign non-privileged access or privileged access for a user or group of users. Non-privileged access allows users to monitor the switch but not configure the switch. Privileged access allows the user to fully manage and configure the switch.

The ExtremeWare software suite implements both Terminal Access Controller Access Control System (TACACS+) and an extended version of the Remote Authentication Dial-In User Server (RADIUS). The RADIUS protocol (IETF RFC 2138) provides an efficient and secure mechanism for authenticating and centrally administering access to network nodes. The ExtremeWare RADIUS client allows authentication for telnet, HTTP and console access to all Extreme switches. As an alternative to privileged and non-privileged categories, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network.

The use of independent access lists based on source IP addresses can also help protect the remote management methodologies used to maintain, update and manage network switching and routing systems. ExtremeWare allows a different access profile to be used for each remote access method (web, SNMP read, SNMP read/write, telnet, SSH2). Additionally, specific services can be completely turned off when not required by the application scenarios.

The following sections provide more detailed information on how Extreme's broadband switching solutions can control access and implement access policies to prevent DoS attacks.

**Controlling Access**

**Management Access**

ExtremeWare supports two levels of management accounts.

**User Account**

A user account allows viewing access to all manageable parameters with the exception of the user account database and SNMP community strings. A user account can also use the ping command to test device accessibility and change the password assigned to the specific account name. For this level of access, the ExtremeWare command line interface prompts end with a (?) sign.

**Administrator Account**

An administrator account allows viewing and changing of all manageable parameters. This account can add or delete users and change the password associated with any account name. For this level of access, the ExtremeWare command line interface prompts end with a (.) sign.
The ExtremeWare™ software suite from Extreme Networks® allows mapping and overwriting of IEEE 802.1p and DiffServ tags to enable DiffServ functionalities that are invisible to external observation. By using these policy mechanisms, system administrators can adjust internal routing control policies for traffic from specific neighboring systems without advertising the actual policies being internally enforced.

The flexibility to differentiate between internal and external DiffServ and IEEE 802.1p criteria can be an effective tool for thwarting a new wave of potential DoS attacks referred to as QoS attacks. In the instances that have appeared so far, these attacks attempt to make use of bogus QoS criteria in order to adversely impact network routing behaviors. It does this by spoofing high-priority traffic classifications and usurping bandwidth away from legitimate QoS classes.

ExtremeWare’s ability to maintain invisible internal DiffServ handling policies enables all Extreme switches to easily ignore, observe or manipulate any DiffServ tags received from a potentially “untrusted neighbor.” The incorporation of network login mechanisms play a key role in reducing vulnerability to DoS attacks. Network login works by using unique usernames and passwords to authenticate users before granting access or passing packet traffic, thereby preventing the risk of pre-authentication DoS assaults.

An authentication key must be generated for each SSH2 session. This can be done automatically by Extreme switches or by the client application. The supported cipher is 3DES-CBC (IETF RFC 1851). The supported key exchange is DSA (IETF RFC 2792).

Simple Network Management Protocol (SNMP) Access

Any network administrator running SNMP can manage Extreme switches if the Management Information Base (MIB) is installed correctly on the management station. Non-privileged access (SNMP read access) allows users on a host to send the switch SNMP get-request and SNMP get-next-request messages. These messages are used to gather information and statistics from the switch. Privileged access (SNMP read/write access) allows users on a host to send the switch SNMP set-request messages in order to make changes to the switch’s configurations and operational settings.

SNMP access allows you to set up different SNMP community strings for both non-privileged and privileged access. The default read-access community string on Extreme switches is public, while the default read/write access community string on Extreme switches is private.

Telnet

Any workstation with a telnet facility should be able to communicate with Extreme switches on the same network as the workstation. While the default setting on Extreme switches accepts telnet sessions, access can be restricted by using an access profile. An access profile accepts or denies a named list of IP addresses and subnet masks.

Secure Shell 2 (SSH2)

FIPS-186 (Federal Information Processing Standards Publication 186) SSH2 is a feature of ExtremeWare that encrypts telnet session data between the switch and a network engineer using SSH2 client software. The ExtremeWare SSH2 switch application is based on the Data Fellows™ SSH2 server implementation. This requires F-Secure® SSH client products from Data Fellows Corporation on the network engineer’s workstation.

Because SSH2 is currently under U.S. export restrictions, before enabling SSH2, you must first obtain a security license (at no extra charge) from Extreme. Go to the Extreme web site at www.extremenetworks.com/go/security.htm and fill out the contact form to indicate compliance or non-compliance with export restrictions. When in compliance, information will be made available to enable the security features.

An authentication key must be generated for each SSH2 session. This can be done automatically by Extreme switches or by the client application. The supported cipher is 3DES-CBC (IETF RFC 1851). The supported key exchange is DSA (IETF RFC 2792).

For more information on Data Fellows’ SSH2 server implementation, visit their web site at www.datafellows.com.

Tailoring routing access policies can ensure “trusted neighbor” relationships to prevent unauthorized access to networks.

The ExtremeWare™ software suite from Extreme Networks® allows mapping and overwriting of IEEE 802.1p and DiffServ tags to enable DiffServ functionalities that are invisible to external observation. By using these policy mechanisms, system administrators can adjust internal routing control policies for traffic from specific neighboring systems without advertising the actual policies being internally enforced.

The flexibility to differentiate between internal and external DiffServ and IEEE 802.1p criteria can be an effective tool for thwarting a new wave of potential DoS attacks referred to as QoS attacks. In the instances that have appeared so far, these attacks attempt to make use of bogus QoS criteria in order to adversely impact network routing behaviors. It does this by spoofing high-priority traffic classifications and usurping bandwidth away from legitimate QoS classes.

ExtremeWare’s ability to maintain invisible internal DiffServ handling policies enables all Extreme switches to easily ignore, observe or manipulate any DiffServ tags received from a potentially “untrusted neighbor.”

Tailored Network Login Provisions

The incorporation of network login mechanisms play a key role in reducing vulnerability to DoS attacks. Network login works by using unique usernames and passwords to authenticate users before granting access or passing packet traffic, thereby preventing the risk of pre-authentication DoS assaults.

By using DHCP to emulate how the dial-up world uses PPP, network login can stop unauthorized access at the edge of the network, and mitigate any negative impact on the network infrastructure. Network login works by having the user’s browser submit a DHCP request to the switch, which captures the required
Even while carrying out wire-speed switching functions at Layer 2, these multi-layer switching systems are able to seamlessly incorporate QoS and access control criteria from Layers 1–4 as well as other sources. Multilayer filtering can easily be set up to scan, classify and selectively handle packets according to criteria such as IP addresses, user names (Layer 7) or IEEE 802.1p criteria and/or DiffServ tag values.

Multi-layer filtering can easily be set up to scan, classify and selectively handle packets according to criteria such as IP addresses, user names (Layer 7) or IEEE 802.1p criteria and/or DiffServ tag values.

This built-in flexibility for layer-independent access control completely separates security decisions from network architecture decisions, thereby enabling network administrators to efficiently deploy DoS preventive measures without being forced into sub-optimal routing or switching topologies. As a result, network administrators and service providers now have the ability to seamlessly integrate policy-based access control criteria throughout their metropolitan, data center or enterprise network environments, whether using complex router-based core services or relatively simple Layer 2 switched local loops.

In addition, wire-speed handling of criteria lookups and dataflow authentication decisions enable DoS countermeasures to effectively take place in the background with little or no performance delays.

**Customizable Filtering and "Trusted Neighbor" Mechanisms**

Another advantage of from intelligent multilayer access control is the ability to easily implement customized filtering actions such as tailoring the granularity of control over the systems’ response to certain criteria. For example, rather than making a simple “pass” or “discard” decision on packets that may be part of a DoS attack, multilayer switching allows the system to push the packets to a specific QoS profile with specified maximum bandwidth limits. This way, the network can be protected from the impacts of DoS attacks while reducing the risk of inadvertently discarding legitimate traffic.

Another advantage of layer-independent access control is the ability to manage and optimize intersystem dataflow by tailoring routing access policies to support “trusted neighbor” relationships between specific systems. In addition, multilayer switching incorporates options that protect internal routing policies from unauthorized exposure and potential subversion.

**Classification + QoS Profile = Policy**

Prior to granting network authorization, the network administrator must use certain protocols to perform the authentication. In today’s networks, TACACS+ and RADIUS protocols are commonly used to provide robust security.

**RADIUS**

The RADIUS protocol was developed as an access server authentication and accounting protocol. RADIUS (IETF RFC 2138) is a mechanism for authenticating and centrally administrating access to network nodes. The ExtremeWare RADIUS client implementation allows authentication for telnet, HTTP or console access to all Extreme switches.

First, a primary and secondary RADIUS server is defined for the switch to contact. When a user attempts to login, the request is sent to the primary RADIUS server and then to the secondary RADIUS server, if the primary does not respond. If the RADIUS client is enabled but access to the primary and secondary server fails, Extreme switches will use its local database for authentication. The privileges assigned to the user (admin vs. non-admin) at the RADIUS server take precedence over the configuration in the local switch database.

The ExtremeWare RADIUS implementation also supports pre-command authentication. Pre-command authentication allows the definition of several levels of user authorization by controlling the permitted command sets based on RADIUS usernames and passwords. This is made possible using the Extreme-modified RADIUS server. The Merit AAA server application is the most commonly used and most publicly available implementation of RADIUS servers. The software is available in compiled format for Solaris™ or Linux™, as well as in source code format.

**TACACS+**

Privileged and non-privileged mode passwords are global and apply to every user accessing a switch from either the console port or from a telnet session. As an alternative, TACACS+ provides a way to validate every user on an individual basis before they gain access to the network. TACACS+ was derived from the U.S. Department of Defense and is described in IETF RFC 1492.

The ExtremeWare version of TACACS+ can be used to authenticate users who are attempting to administer the switch. The TACACS+ protocol is used to communicate between the switch and an authentication database. With TACACS+ enabled, Extreme switches will prompt the user for a username and password. Then, the switch queries the TACACS+ server to verify the supplied information. The TACACS+ server typically runs on a UNIX workstation and quite a few implementations are available in the public domain.
In addition to authenticating users, the Extreme TACACS+ implementation delivers the mechanism to perform authorization and accounting similar to RADIUS.

**Differences between RADIUS and TACACS+**

Although these two protocols provide similar functionality, they have several key differences.

*Transport Mechanism*

The most fundamental difference between TACACS+ and RADIUS is the network transport protocol that each one uses. The RADIUS protocol uses UDP to exchange information between the NAS and the access control server, whereas TACACS+ uses the Transmission Control Protocol (TCP).

TCP is a connection-oriented transport protocol, whereas UDP offers best-effort delivery. RADIUS utilizes additional, programmable variables to control factors such as retransmit attempts and timeouts in order to compensate for the best-effort transport provided by UDP. TACACS+ does not need these extra variables because connection issues are handled transparently by the TCP protocol.

TCP provides a separate acknowledgment via a TCP acknowledgment packet when a request has been received by the access control server within an acceptable network round-trip time. This acknowledgment occurs regardless of the congestion of the access control server.

TCP provides immediate indication of an unavailable server. Long-lived TCP connections will even reveal servers that go down and then come back up. UDP is unable to discriminate between a down server, a slow server and a non-existent server.

Using TCP keep-­­­-­­­-alive, server crashes can be detected out of band with actual requests. Connections to multiple servers can be maintained simultaneously and messages need to be sent only to servers that are known to be up and running. TCP provides a stable foundation that is scalable for all types of networks.

*Confidentiality*

RADIUS encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is in the clear. Other information such as username, authorized services and accounting can be captured by a third party, making RADIUS networks potential targets of hackers using session capture and replay attacks.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether or not the body is encrypted. Normal operation fully encrypts the body of the packet for more secure communications.
Distribution of Functionality
The RADIUS protocol combines the processes of authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication and authorization functions difficult. The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, as seen in many service provider networks.

During a session, if additional authorization checking is required, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This feature provides greater control over the commands that can be executed on the access server while decoupling authorization from the authentication mechanism. TACACS+ is thus more appropriate to use when multiple authentication methods in a complex network are deployed.

Multiprotocol Support
RADIUS has limited support for protocols other than TCP/IP. For example, RADIUS does not natively support the following protocols:

- AppleTalk Remote Access (ARA)
- NetBIOS frame protocol control
- Novell Asynchronous Services Interface (NASI)
- Packet Assembler/Disassembler (PAD) connection

These protocols are natively supported by TACACS+.

Access Policies
Once access to the network is authenticated, the next step is to protect networked resources. These resources or nodes are where intellectual property and confidential information reside. Access policies are a general category of preset decision making rules that impact forwarding and route forwarding decisions. Access policies are used primarily for security and QoS purposes. There are three categories of access policies: access lists, routing access policies and route maps.

Adverse Impacts of DoS Attacks
Using relatively simple assault methods, DoS attacks can completely disable target systems or even disrupt entire networks by not allowing them to function properly. A DoS attack can bring entire organizations to a complete standstill, thereby costing millions of dollars in lost revenue and/or productivity.

For example, some recent high-profile DoS attacks have targeted major Internet portals or e-commerce sites by disabling web site access for extended periods of time and resulting in loss of revenue and credibility. In other cases, DoS attacks have been aimed at disrupting and disabling major Internet service providers (ISPs), causing widespread havoc among all users across large geographic areas.

Implementing Countermeasures Against DoS Attacks
Effective protection against DoS attacks involves taking countermeasures at all levels across the inter-networking infrastructure, including taking specific actions at the LAN level and addressing broader issues at the network transport level.

LAN Level Issues
At the LAN level, system administrators can take a number of preventive measures to guard against the disabling effects of DoS attacks. These preventive measures range from maintaining solid overall administrative and security procedures to implementing specific safeguards targeted at countering each of the various types of DoS attacks.

For example, while it is virtually impossible to completely eliminate spoofing of IP packets, system administrators can effectively reduce the risk of internally fueled spoofed IP attacks by instituting filtering actions that restrict the flow of data input if they have source addresses from within the internal network. In addition, administrators can reduce the risk of being used as an intermediary in spoofed IP DoS attacks by installing filters to restrict the external flow of IP packets with source addresses that don’t originate within the internal network.

Other methods associated with specific types of DoS attacks may include turning off or restricting specific services that might otherwise be compromised or subverted. For instance, UDP services could be restricted for use only within the internal network, thus keeping UDP available for network diagnostic purposes only. This prevents its unauthorized use for UDP flooding attacks.

Unfortunately, such restrictive measures must also be weighed against the impact they may have on legitimate applications, such as RealAudio that uses UDP as the transport mechanism. If attackers are able to intimidate victims into not using beneficial IP services or legitimate applications, to some extent, they have accomplished their objectives.
Access Lists

IP access lists consist of IP access rules that are used to perform packet filtering and forwarding decisions on incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order. Then, it is either forwarded to a specified QoS profile or dropped. Using access lists has no impact on switch performance. Access lists are typically applied to traffic that crosses Layer 3 router boundaries, but it is also possible to use access lists within a Layer 2 VLAN.

Each entry that makes up an IP access list contains a unique name. It can also contain an optional, unique precedence number. The rules of an IP access list consist of a combination of the following six components:

- IP source address and mask
- IP destination address and mask
- TCP or UDP source port range
- TCP or UDP destination port range
- Physical source port
- Precedence number (optional)

When a packet arrives on an ingress port, the packet is compared with the access list rules to determine a match. When a match is found, the packet is processed. If the access list is of type deny, the packet is dropped. If the list is of type permit, the packet is forwarded. A permit access list can also apply a QoS profile to the packet.

Routing Access Policies

Routing access policies control the advertisement or recognition of routing protocols such as RIP, OSPF or BGP. Routing access policies can be used to “hide” entire networks or to trust only specific sources for routes or ranges of routes. The capabilities of routing access policies are specific to the type of routing protocol involved. However, they are sometimes more efficient and easier to implement than access lists.

Route Maps

Route maps can be used to control the redistribution of routes between two routing domains and to modify the routing information that is redistributed. Route maps are used in conjunction with the match and set operations. A match operation specifies criteria that must be matched. A set operation specifies a change that is made to the route when the match operation is successful. Route maps are used to modify or filter routes redistributed into BGP. They are also used to modify or filter the routing information exchanged with BGP neighbors.

Teardrop Attacks

Teardrop attacks exploit IP mechanisms involved in the reassembly of packets that have been disassembled for efficient transmission. In normal practice, each packet fragment looks like the original IP packet with the exception of an offset field that specifies which bytes of the original packet are included (i.e. bytes 400 through 600), thereby enabling the receiving system to reassemble all of the data in the proper sequence. By purposely creating packet fragments with overlapping offset fields, these types of attacks make it impossible for the victim’s system to correctly reassemble the packet fragments, which can sometimes cause the destination system to hang, crash or reboot.

Smurf Attacks

Smurf attacks take advantage of direct broadcast addressing mechanisms by spoofing the target system’s IP address and broadcasting Internet Control Message Protocol (ICMP) ping requests across multiple subnets. This attack clogs the victim’s network with bogus ICMP echo requests and responses, thereby making it unavailable to legitimate traffic. All intermediary systems that are co-opted or drawn into the echo-response cycle become victims of this attack, both suffering from and contributing to overall network congestion.

Oversized Packet Attacks

Sometimes referred to as “ping of death” attacks, oversized packet attacks exploit a known bug in some TCP/IP implementations by using the ping utility to send packets that exceed the maximum 65,536 bytes of data allowed by the IP specification. When it first emerged, this type of attack caused crashes, hangs or reboots in victim’s systems. However, most operating system vendors have now addressed this issue with software updates that enable smooth disposition of oversized packets.

UDP Flood Attacks

This DoS attack takes advantage of User Datagram Protocol (UDP) mechanisms by creating bogus UDP connections between unsuspecting systems. When a connection is established between two UDP services, each of which produces output, the combined effects can produce a very high number of packets and result in denial of service to legitimate users. In UDP flood attacks, the intruders use forged UDP packets to connect the echo service on one machine to the chargen service on the other machine, causing the two machines to consume all available bandwidth on the connection between them.
The Rising Challenges from Denial-of-Service (DoS) Attacks

DoS attacks are typically aimed at servers connected to the Internet with the intent of degrading or disabling the systems to the extent that the services become unavailable to legitimate users. Instead of attempting to hack into the target systems to access confidential data, DoS attacks focus on overwhelming the systems with bogus and/or defective traffic that undermines their ability to function normally.

Modes of Attack

DoS attacks come in a variety of forms and aim at a variety of services. There are three basic types of attacks:

- Consumption of scarce, limited or non-renewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

Some DoS attacks can be executed with limited resources against a large, sophisticated web site or network. This type of attack is sometimes called an asymmetric attack. For example, an attacker with an old PC and a slow modem may be able to disable faster and more sophisticated machines or networks. Many DoS attacks have also been referred to as distributed because they make use of a wide array of individual computers that have been surreptitiously co-opted to fire DoS traffic from many different directions at the target system or network.

Trends in DoS Attacks

Typical examples of recent trends in DoS attacks have included:

- Attempts to “flood” a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person

Specific Types of DoS Attacks

SYN-ACK Attacks or TCP-SYN Flooding

A SYN-ACK attack exploits the TCP/IP mechanism by using a three-way handshake in order to establish a communications link. By only initiating the handshakes and not responding to the server’s acknowledgements, SYN-ACK attacks force the server to store huge numbers of acknowledgement packets in its backlog queue, with the objective of overflowing the queue and disabling the server’s ability to issue any more acknowledgements. One variation of SYN-ACK attacks actually spoofs the IP address of the victim’s system so that the system is taken out of service by talking to itself.

The entries in a route map are processed in the ascending order of the sequence number. Within the entry, the match statements are processed first. When the match operation is successful, the set and go-to statements within the entry are processed and the action associated with the entry is either applied, or the next entry is processed. If the end of the route map is reached, it is implicitly denied. When there are multiple match statements, the primitive match-one or match-all in the entry determines how many matches are required for success. When there are no match statements in an entry, the entry is considered a successful match.

Forwarding-Controls and Load-balancing Methods

Because some DoS attacks result from intruders understanding your routing policies, it is also important to maintain tight controls over basic policy disciplines such as IP-broadcast forwarding controls, ICMP and IP option response controls. Forwarding criteria can also be tailored to provide unidirectional session control, where broadcast sessions can be restricted to occur only from within the network and not from external sources.

In addition, the intelligent use of server load-balancing based on multilayer switching can help forward legitimate traffic only within the network and protect internal servers from the impact of DoS assaults that may penetrate other defense mechanisms.

Rigorous DoS Stress Testing

The final area of critical importance is ensuring that the switching and routing systems themselves undergo rigorous design tests to ensure reliability and robustness, even when directly subjected to the most demanding DoS stress testing. Achieving these objectives depends on the robustness of the system architecture and is ultimately tested using real-world DoS attacks.

All Extreme switches and the ExtremeWare software suite share the same consistent architecture to provide end-to-end simplicity and maximum resiliency by incorporating critical features such as redundant physical (PHY) connections, non-blocking wire-speed processing, sub-second failover/failback mechanisms and automatic load-sharing.

Extensive proof-of-design testing of Extreme switches has been conducted to ensure immunity against the full spectrum of DoS attack modes listed.
All testing is conducted up to full line-rate speeds while the pass criteria requires that the system both successfully survives the attack and is able to log and report the attack.

The Bottom Line

It is clear that the wave of DoS attacks will continue to pose as a significant threat to all businesses whether you are a service provider, e-business or a big enterprise. As new countermeasures are developed, new DoS attack modes undoubtedly will also emerge. Ensuring high resiliency and high performance in public and private networks will require concerted efforts from administrators, service providers and equipment manufacturers.

Use of tightly controlled management access to systems and intelligent management of routing policies are critical in laying the groundwork for building a first line of security against DoS attacks. Network switching and routing equipment also need to provide a broad adherence to standard security methodologies and mechanisms to provide system administrators with the flexibility to effectively manage and scale their network infrastructures in a secure manner.

From a network infrastructure standpoint, the ability to prevent and withstand DoS attacks depends heavily on deploying advanced hardware and software capabilities embodied in leading edge switching and routing system architectures. Key factors such as multilayer switching with layer-independent access-control decisions enable the network transport infrastructure to automatically recognize and fend off DoS attacks while continuing to maintain wire-speed performance.

Furthermore, the ability to tailor filtering criteria, establish intersystem trusted-neighbor relationships and institute user-level network login mechanisms all enable today’s networks to quickly and efficiently respond to the ever-changing nature of DoS attacks. Ultimately, the network infrastructure must be both robust enough to survive direct DoS attacks and extensible enough to adapt and embrace new defenses against emerging and unanticipated attack modes.