Ryan Dusek
GSEC Version 1.2f
28 November 2001

Basic Cisco Access Control Lists

Welcome to an introduction of the basic Cisco access control lists. My goal of this paper is to introduce you to some of the most common types of control lists used in the Cisco router environment. I will be covering access control pertaining to static routing, standard, extended, time based and dynamic access control lists. In each of the sections I will briefly mention what the control does for the network and define the command structure. A sample network diagram, which will be related with the subsequent example explanation, will follow. Finally, I will point out some of the advantages and disadvantages associated with each list.

This paper is intended for the beginning network administrators and others who are interested in learning about Cisco access control lists. Keep in mind that this paper will not cover any one style of access control in-depth, nor will it cover all the different access control list types. Lastly, for the sake of ease, all examples will be based on the TCP/IP architexture. I hope you enjoy the paper and that you come away with a new appreciation and understanding of Cisco access control lists.

The first step in understanding access control lists would be to know the rules. All access lists follow these simple rules.

1. There is an implicit deny for all packets at the end of the access control list.
2. If an access control list is present, then the list applies to all packets.
3. No more than one access list may apply to either the inbound or outbound side of an interface.
4. Access lists may apply to inbound or outbound traffic.
5. Packets are compared to the access list in a sequential method, starting from the first line. When the packet matches an access control parameter, then the packet is dealt with in the appropriate manner. Refer to rule one if no matches are found.

Now that we have our access control rules established, lets examine our first style of access control.

Static Routes

I start this piece with the most rudimentary access control list. Static routing is probably the first and most simplistic access control list available to any router. By diverting packets from a destined network, static routes use the very essence of the routing layer to provide the fundamentals in access control. For example, if an administrator wishes to block traffic to or from a host or network, then the administrator could simply add a static route to block all packets from entering or leaving the network.

In another situation the administrator may choose to route all packets destined to an identified network into a bit bucket or null interface. The null interface is a virtual destination within the router that informs the router to drop the packet.

Command

ip route *network-address network-mask destination-ip-address* [**null**] *hop-count*

ip route	The Cisco command used to indicate a static route.
network-address	The destined network of the packet
network mask	The subnet of the destined network
destination IP address	The address of the next router. The interface name can also be used if the next route is on the router.
null	Indicates the null route
hop count	The number of hops to the next router

Diagram

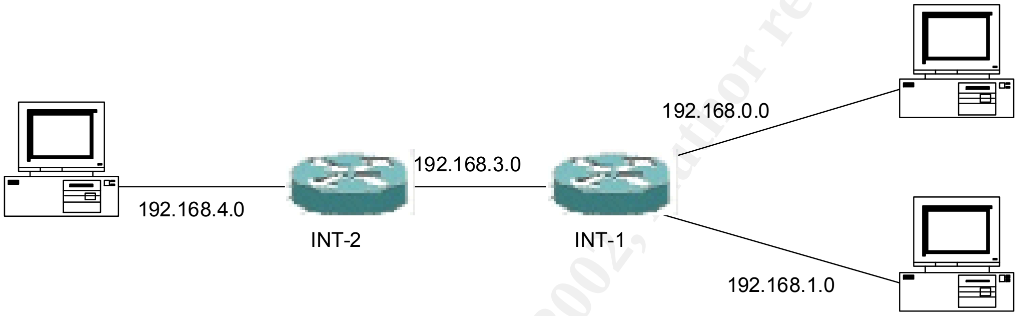

Figure 1

Example

Using the diagram above we will assign static routes to the INT-2 and the INT-1 routers and examine how using a static route can help control access. Let’s assume that all networks in the examples are class C with 254 hosts available. Let’s set the parameters to our situation:

- The 192.168.3.0 network is only a connection between the two routers and does not contain any hosts.
- The hosts on the 192.168.0.0 network do not need access to the 192.168.4.0, but they do need access to the 192.168.1.0 network.
- Hosts on the 192.168.1.0 network need access to all the networks.
- Packets from the all other networks are not allowed to access the 192.168.0.0 network.

If we set the static routes on INT-1 to reflect the following:

```
ip route 192.168.4.0 255.255.255.0 192.168.3.2 1
ip route 192.168.1.0 255.255.255.0 ethernet 0
ip route 192.168.0.0 255.255.255.0 ethernet 1
```

Now any packet coming into the INT-1 router will be routed to the correct destination. For example, if a packet originates in the 192.168.1.0 network and is destined for 192.168.0.0 network, then the router knows to route the packet on the line connected to the ethernet 1 interface. This is an example of an open router, which does not control access to any networks. Remember that we wanted to let the 192.168.1.0 network have access to the 192.168.0.0 network, but we don't want the 192.168.4.0 network to have access to the 192.168.0.0 hosts. This is where we need to configure the other router.

Let's set the following static routes on the INT-2 router and see what happens.

```
        ip route 192.168.1.0 255.255.255.0 192.168.3.1 1
        ip route 192.168.4.0 255.255.255.0 ethernet 0
        ip route 192.168.0.0 255.255.255.0 null 0
```

If we trace the path for a packet originating from the 192.168.4.0 network destined to the 192.168.1.0 network, we see that the packet will enter router INT-2. The static route will direct the packet to 192.168.3.1, which is the IP address of INT-1 router. INT-1 will look in the routing table and determine that it needs to route the packet on ethernet 0 interface. The access control occurs when a packet originating on the 192.168.4.0 network attempts to forward to the 192.168.0.0 network. The INT-2 router references its routing table and sends the packet to the null route. The packet never reaches router INT-1 and is dropped.

I think I know what question you have in mind. If INT-1 will allow packets to enter the 192.168.4.0 network, then will a packet originating from a 192.168.0.0 network route to the 192.168.4.0 network? The answer is yes, but the host on the 192.168.0.0 network will never receive a reply from the destination host on the 192.168.4.0 network. Remember, the reply packet would be destined for the 192.168.0.0 network and INT-2 router would drop the packet. Sounds like a terrible way to control access, huh? Exactly the point, hence the popularity of access control lists. Before we look at the access control lists, let's examine some of the advantages and disadvantages of static routes in access control.

Advantages

Using static routes to control access does have some advantages. First, configuring static routes is probably by far the easiest. Secondly, one simple command can address all packets entering and leaving the router. Finally, the router is performing exactly what it is designed to do, route packets. By routing packets through a null route, the router can greatly reduce CPU cycles. Instead of using CPU cycles breaking down a packet and building it back up, the packet is disassembled and dropped.

Disadvantages

Static routing has its share of disadvantages too. First, this type of access control is good for small environments. Configuration and maintenance of static routes in larger environments, where topologies are changing and routes periodically breakdown can cause headaches for system administrators. In essence, static routing is not very scaleable. Secondly, static routes do not provide granular control of access. There are situations when we do want certain packets to enter or leave our networks.

Standard Access Control List

If you are a brand new system administrator or have been doing system administration for years, but you never worked in routers, then the standard access control list is the perfect place for you to start. Standard access control lists block or permit packets based solely on their source address. Configuration is simple and easy to follow. Furthermore, all other access control lists use the command as the foundation to create complex access controls.

Command

access-list *access-list-number* {**permit** | **deny**}*source source-wildcard*

access-list	The Cisco command to indicate an access control list.
access list number	An assigned number to the access list. This allows several access list rules to occupy the same list. See Appendix A for the list range.
permit | deny	Sets the parameter on the access list to permit or deny the packet from traversing the router.
source	The source IP address of the packet.
source wildcard	Used to define the number of hosts for the source IP address. This number defines the hosts for a network. For example 0.0.0.255 defines all hosts on the class C network.

ip access-group *access-list-number* {**in** | **out**}

ip access-group	The Cisco command used to represent the access control list for the interface
access list number	An assigned number to the access list.
in | out	Sets the parameter on the access control list as to whether the access list should be applied to packets entering or leaving the interface.

Diagram

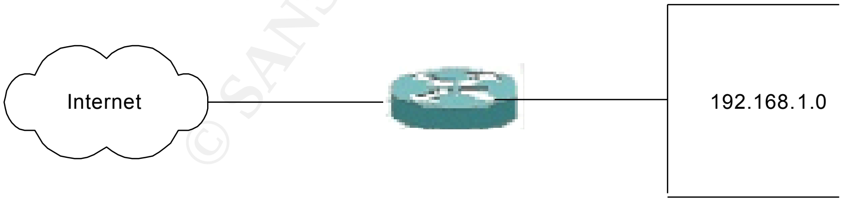

Figure 2

Example

In order to use access control lists, we must first define the list with an appropriate identifier. Referencing the Access Lists Numbers table in Appendix A, we see that for an IP standard access list we can use the numbers ranging from 1 to 99.

For our example above I will create a list using the number 2. Now let's set up our access control list.

```
access-list 2 permit 10.1.0.0 0.0.0.255
access-list 2 permit 10.1.2.10 0.0.0.0
access-list 2 deny 10.1.2.0 0.0.0.255
access-list 2 deny any
```

Our next step is to apply the access control list to an interface and determine the direction that we want the list to apply to the packets. For example, we would want the access control list to apply to the outside interface. Therefore under the configuration for the interface we would put the following command.

```
ip access-group 2 in
```

This command assigns the standard IP access list number 2 that we defined earlier to the interface. Additionally, we added the command 'in' at the end. This tells the router that we want to inspect all incoming packets. If we applied 'out' to the end of this command, then the router would only apply the access list to packets leaving the interface.

Now that we have the access list configured and applied to an interface, let's follow a few packets to see how the access control functions. Starting with a packet containing a source address of 10.1.0.5 and destined to a host internally to us, we see that the router will inspect the packet and compare it against the access list. Starting from the top and referencing the first line, the router determines that the packet is permitted to pass.

Let's try another packet. This one will originate from 10.1.2.8 and be destined for our internal network. The router will receive the packet and reference the list. Starting at the first line, the router notes that the first line does not apply and continues to the next. The wildcard 0.0.0.0 in the second line indicates that only host 10.1.2.10 is permitted through the router and therefore does not apply. Checking the third line, the router determines that the packet is denied access and will drop the packet.

The last line in the list is used as a catch all for anything that we may have missed. It will deny all packets that do not meet the parameters set in the list. Remembering that there is an implicit 'deny all' for access control lists, we should conclude that this statement is not needed. This is exactly true, however, administrators will typically add the statement for others to understand the flow of the access list. Now that we have an understanding of how standard access lists work, let's examine some of the advantages and disadvantages before moving on to extended access control lists.

Advantages

Standard access control lists are the easiest true access control lists to configure. In addition, managing the lists based on the source IP address can significantly speed up configuration and maintenance of access control. Finally, standard access control lists work extremely well with beginning system administrators.

Disadvantages

Some of the advantages could also be disadvantages, such as the access control based on source address. There isn't really a good way to limit traffic a specific host. Complementary to the last point, standard access lists cannot filter traffic based upon any protocols. If the source address is allowed to pass packets through then anything can enter the network. To stop this from happening, we must move on to extended access control lists.

Extended Access Control List

Configuring standard access control lists is easy, but what if you want more control over what types of packets can enter or leave your network. Extended access control lists provide the flexibility that we are looking for to accomplish these tasks. Additionally, extended lists will become the basis for creating time based access control lists, dynamic access control lists, reflexive access control lists and context based access control lists. Each one just adds additional parameters and options to the basic extended access control list.

How is it that extended control lists can provide greater control over packets? Unlike the standard access control lists, which filter packets based on source address, the extended lists can filter packets on the source and destination addresses, protocol and port numbers. This provides a multitude of checks that a packet can be identified. Let's take a look at the command line and some of the definitions.

Command

access-list *access-list-number* {**permit** | **deny**} *protocol source source-wildcard*
destination destination-wildcard [**eq** [*port*]]

access-list	The Cisco command to indicate an access control list.
access list number	An assigned number to the access list. This allows several access list rules to occupy the same list. See Appendix A for the list range.
permit | deny	Sets the parameter on the access list to permit or deny the packet from traversing the router.
protocol	Indicates the name or number of the protocol. For example the protocol may be icmp, ip, tcp, udp, etc or a number from 0 to 255.
source	The source IP address of the packet.
source wildcard	Used to define the number of hosts for the source IP address. This number defines the hosts for a network. For example 0.0.0.255 defines all hosts on the class C network.
destination	The destination IP address of the packet.
destination wildcard	Used to define the number of hosts for the destination IP address.
eq	Cisco keyword for equivalent.
port	Port number or name. For example 'http' is port 80.

Diagram

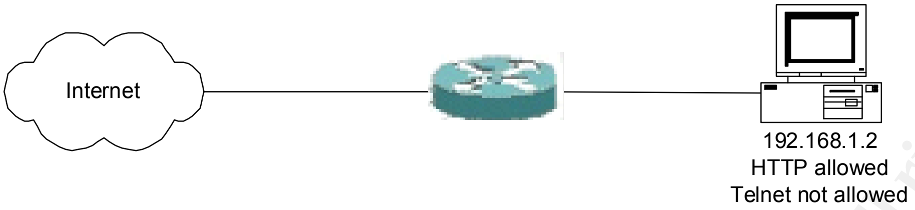

Figure 3

Example

Similar to the standard access control list, we must first define the list with an appropriate identifier. Referencing the Access Lists Numbers table in Appendix A, we see that for an IP extended access list we can use the numbers ranging from 100 to 199. For our example above I will create a list using the number 100. Again, we set up the access control list, but you will see that there are many more variables added to our list.

```
access-list 100 permit tcp any 192.168.1.100 0.0.0.0 eq http
access-list 100 permit telnet 10.1.0.9 0.0.0.0 192.168.1.100 0.0.0.0 eq telnet
access-list 100 deny telnet  any  host 192.168.1.100 eq telnet
access-list 100 deny any any
```

Once again we assign the control list to an interface and determine the direction that we want the list to apply to the packets. From our diagram above, we see that we want to once again put the list on the outside interface to catch all packets entering out internal network.

```
ip access-group 100 in
```

Let's take a different approach and walk down the list. The first line uses the word 'any' to represent the source address. Cisco routers take the word 'any' to represent all addresses and all wildcards. The destination is set to only the host 192.168.1.100. You also see that the port is set to 'http' and can probably already assume that the machine is hosting a web page. It is this next part that I want you to really pay attention. Notice that the protocol is set to tcp. I do this because 'http' requires that the protocol be set to tcp. If for example the protocol was set to ip instead of tcp, then the all packets for the web site would fail this control entry and never reach the web server. This is where most of the mistakes occur when setting up an extended access control list. Just be careful when you make extended access control lists that you verify your protocol with your port.

The second entry allows only the host 10.1.0.9 to telnet to 192.168.1.100. On the other hand the third entry will prevent all other hosts from performing a telnet into 192.168.1.100. Notice how I was able to use the term 'host' in my third entry. 'Host' indicates that the destination address is the host. This seems like it doesn't follow the prescribed command sequence, but if you remember in the introduction, I mentioned that Cisco command lines could be somewhat lenient in their acceptance of commands. I present this so that you can get used to seeing different formats for the same commands. Finally, this brings us to our last statement, which again is the catch all for anything we might have missed.

I am sure you could follow packets through this control list by now. If you missed how this works, then re-read this section and keep in mind that you start at the beginning of the access list and work your way down until you find an entry that works for the packet. At this point you drop out of the access control list.

Advantages

The biggest advantage of an extended access control list is the ability to distinguish and filter packets based on source address, destination address, protocol and port number. This gives greater flexibility to the system administrator in designing the network.

Disadvantages

Unfortunately, once you start adding more and more options to an access control list, you run the risk of introducing more complexity. Extended access lists can sometimes be difficult to configure and often times frustrating. Furthermore, careful maintenance of the lists should be applied so nothing unexpected can traverse the router.

<u>Time Based Access Control List</u>

We'll start with an easier extended access control lists. Cisco has incorporated a way to allow packets to traverse routers based on the day and time. You might be thinking to yourself, "Why would you ever allow access during one time frame as opposed to another?" That is a great question, why would you. Here are some answers that I came across. Maybe you want to allow people to download large files when network response times aren't in demand. Maybe, you want to let video-conferencing to take place during certain times. Or maybe, you want to open the network for morale purposes and allow employees to play games on the weekend. The point is that whether there is a good reason or not, Cisco provides you with the means to setup a time based access control list.

Command

time-range *range-name*

time range	Cisco keyword used to identify a name associated with a time based access control list
range name	The name associated with the time range

periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

periodic	Cisco keyword used to identify a period of time

day of the week	A day selection to determine which days the access control list will apply. Keywords could be “Monday”, “Daily”, “Weekday”, etc
hh:mm	A time period to determine what times the access control list will apply

access-list *access-list-number* {**permit** | **deny**} *source source-wildcard* [**eq** [*protocol*]] [**time-range** *range-name*]

access-list	The Cisco command to indicate an access control list
access list number	An assigned number to the access list. This allows several access list rules to occupy the same list. The list may range from 100 to 199.
permit | deny	Sets the parameter on the access list to permit or deny the packet from traversing the router.
source	The source IP address of the packet
source wildcard	Used to define the number of hosts for the source IP address. This number defines the hosts for a network. For example 0.0.0.255 defines all hosts on the class C network.
eq	Cisco keyword for equivalent.
protocol	Indicates the name or number of the protocol. For example the protocol may be icmp, ip, tcp, udp, etc or a number from 0 to 255.

Diagram

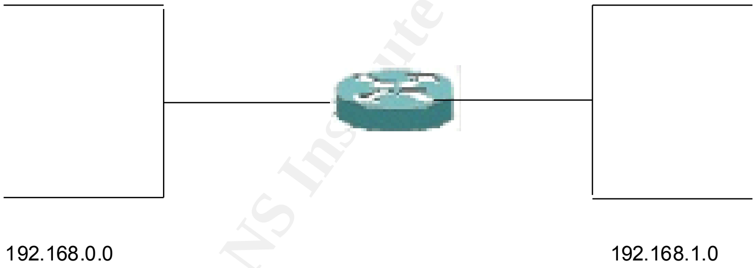

Figure 4

Example

The first step in setting up the time based access control list is to synchronize all the router clocks. This is probably best done using the network time protocol (NTP). Next, we need to establish an identifier for our time range and the period associated with that identifier. The time range will be called ‘playtime’ and it will start every Friday at 5:00 pm and end every Monday at 8:00 am.

```
time-range playtime
periodic Friday 17:00 to Monday 08:00
```

Next we will associate an extended access list for the time range. Notice how I needed to reference the access list number for IP extended access lists. Finally, I assign the access list to an interface and provide direction for packet inspection.

```
access-list 100 permit any any eq tcp time-range playtime
ip access-group 100 in
```

As you can see we have established a time period that will allow any tcp traffic originating from any host and destined to any host to traverse the router. Obviously, this isn't the best scenario to have for time based access control, but it does show that you need to be careful when configuring access control lists.

Advantages

I've already mentioned the advantages of using a time based access control list, but I will re-affirm those ideas again. First, you now have the flexibility to allow or deny traffic based on a time frame. For example, you could shutdown access to the entire network over the weekend and have it automatically re-open on Monday morning. Another advantage is that you can improve employee morale by allowing them to download large files or play network games when demand for network resources is low.

Disadvantages

One of the major disadvantages of using time based control lists is that you could open security holes within your network if you are not careful as to what you allow through the router. Another downside is that you may limit user freedom to specific time periods and end up bringing morale down. This could cause headaches for you or the help desk.

Dynamic Access Control List

Time based access control lists are great tools when you want to open up traffic through the router at certain times, but what if you have personnel that need access through the router at random intervals? This is where dynamic access control lists can help out. Dynamic lists solve the above problem by allowing a user to signal the router that access is needed. In turn, the router will grant the access and then close the route once access requirements have ceased. Let's take a look at the command and jump into an example.

Command

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]]
{**permit** | **deny**} *protocol source source-wildcard destination destination-wildcard*

access-list	The Cisco command to indicate an access control list
access list number	An assigned number to the access list. This allows several access list rules to occupy the same list. The list may range from 100 to199.

dynamic	Cisco keyword for the router to understand that this will be a dynamic access control list
dynamic name	Assigns a name identifier to the dynamic control list
timeout	Cisco keyword used to set the idle time length before disabling the access control list
minutes	The number of minutes that a user can be idle before the timeout parameter removes the access
permit | deny	Sets the parameter on the access list to permit or deny the packet from traversing the router.
protocol	Indicates the name or number of the protocol. For example the protocol may be icmp, ip, tcp, udp, etc or a number from 0 to 255.
source	The source IP address of the packet
source wildcard	Used to define the number of hosts for the source IP address. This number defines the hosts for a network. For example 0.0.0.255 defines all hosts on the class C network.
destination	The destination IP address of the packet
destination wildcard	Used to define the number of hosts for the destination IP address.

Diagram

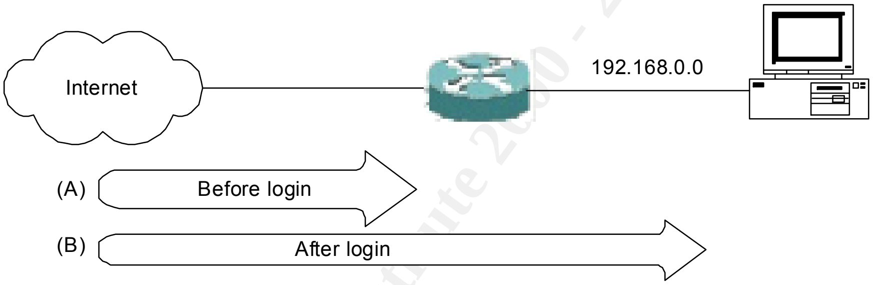

Figure 5

Example

The first step in creating a dynamic list is to incorporate method for the user to inform the router when access will be needed. We accomplish this by entering an extended access control list to allow users to telnet into the router.

```
access-list 100 permit telnet any 192.168.0.1 0.0.0.0 eq telnet
```

Our next step is to establish a method for the router to open a control list. Using the account identifier ‘surfing’ as the login parameter, a user logs into the router through the already established telnet interface. The router will authenticate the user and open access to permit IP traffic from any host to any host.

```
access-list 100 dynamic surfing timeout 10 permit ip any any
```

```
access-list 100 deny any any
```

Don’t forget that we need to assign the access list to an interface.

```
ip access-group 100 in
```

Finally, we want to authenticate the account surfing to access the router. We accomplish this by assigning a password to the account ‘surfing’.

```
Username surfing password theinternethighway
```

All a user has to do to gain open access through the router is telnet into the router and authenticate using the ‘surfing’ account. Besides allowing the traffic to flow through the router, this action will also start an idle timer. The router monitors the network traffic from the user machine to the router. As traffic remains idle, the timer will countdown until it eventually reaches the prescribed 10-minute threshold we assigned in the access control list. At this point the router will once again disable the control list and deny any further packet flow. This is a wonderful mechanism to allow users to dictate when they need access through the router while at the same time providing security by closing off the connection without any user intervention.

The diagram above depicts packet traffic (A) before the access control list is open and (B) When the user authenticates through the telnet interface.

Advantages

Allowing users to dictate when they access through the router is required can provide less management on the administrator’s part and is probably the biggest advantage of a dynamic list. Additionally, having the ability to automatically close idle connections will aid in the security.

Disadvantages

How many users do you really want to telnet into your router? In most cases, the answer is none. However, dynamic lists require the authentication to open the route. Another disadvantage is that to provide a high degree of security, the administrator needs to already know the type of traffic a user would need to pass through the router. Default configurations like the example above, will leave the router vulnerable during open periods.

Reflexive and Context Based Access Control (CBAC) Lists

This paper focused on the basic Cisco access control lists, but I wanted to take a moment and mention a little about two of the more advanced access control lists. The first of these two is the Reflexive access control list, which uses two extended access control lists working together to create the same effect as dynamic access control list, only without any user authentication. As you can imagine this is probably the biggest advantage in using reflexive over dynamic access control lists. However, reflexive lists do have the disadvantage of not being able to handle applications that require multiple channels. To overcome this limitation, Cisco comes to our rescue with probably their most advanced access control list, Context Based Access Control (CBAC).

CBAC lists were designed to handle access control for applications dealing with multiple channels. Additionally, as part of the IOS Firewall feature set, CBAC has the ability to perform several other tricks to include support for the Cisco IOS Firewall Intrusion Detection System, filtering at the application layer of the OSI model and creating real-time alert notification. These are just some of the advantages. The downside to CBAC is the learning curve to fully master the access control list creation. Worst yet, CBAC only supports a handful of protocols for applications, which means that CBAC may not work for some applications. Furthermore, CBAC and IPSec tend to not play very well together. But with every access control list, you will have to weight the good with the bad and determine which style fits your network needs.

Summary

I didn't mention all of the access control list types from Cisco, but I have tried to familiarize you to the most common styles. My goal was to introduce you to the topic of access control lists and hopefully ignite an interest in providing security at the router level. I highly recommend taking the next step and looking into more aspects of network security to include securing a router, Cisco Firewall Feature Set and preventing Denial of Service Attacks.

1. Cisco Systems. URL:
   http://www.cisco.com/

2. Cisco Systems. "Configuring Access Control." URL:
   http://www.cisco.com/univercd/cc/td/doc/product/l3sw/8540/12_1/lhouse/sw_confg/8500acl.htm

3. Cisco Systems. "Access Control List: Overview and Guidelines." URL:
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdacls.htm

4. Cisco Systems. "The Cisco IOS Firewall Feature Set and Context-Based Access Control." URL:
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/firewall.htm

5. Lindsay, Paul. "Cisco Reflexive Access Lists." URL:
   http://www.sans.org/infosecFAQ/firewall/reflex.htm (10 May 2001)

6. Mason, Andrew and Newcomb, Mark. Cisco Secure Internet Security Solutions. Indianapolis: Cisco Press, 2001.

7. Leinwand, Allen and Pinsky, Bruce. Cisco Router Configuration 2nd Ed. Indianapolis: Cisco Press, December 2000.

8. Wenstrom, Michael. Managing Cisco Network Security. Indianapolis: Cisco Press, April 2001.

Appendix A

The following is a list of protocols and their representative range for access control lists.*

Protocols with Access Lists Specified by Numbers Protocol	Range
IP	1 to 99 and 1300 to 1999
Extended IP	100 to 199 and 2000 to 2699
Ethernet type code	200 to 299
Ethernet address	700 to 799
Transparent bridging (protocol type)	200 to 299
Transparent bridging (vendor code)	700 to 799
Extended transparent bridging	1100 to 1199
DECnet and extended DECnet	300 to 399
XNS	400 to 499
Extended XNS	500 to 599
AppleTalk	600 to 699
Source-route bridging (protocol type)	200 to 299
Source-route bridging (vendor code)	700 to 799
IPX	800 to 899
Extended IPX	900 to 999
IPX SAP	1000 to 1099
Standard VINES	1 to 100

Extended VINES	101 to 200
Simple VINES	201 to 300

*This table was taken from Cisco Systems. “Access Control List: Overview and Guidelines.” Figure 15.