

# The Changing Face of Network Security Threats

Brian Floyd, [brianfloyd@ieee.org](mailto:brianfloyd@ieee.org) - Member IEEE, SCTE

*Abstract*— Security threats abound in today’s digital age and along with this, network administrators need to adhere to industry best practices when it comes to their internet infrastructure. Security threats arise almost on a daily basis and an aware administrator needs to be able to understand the types of risks and be able to respond quickly and appropriately. This paper discusses the basics of different security and network threats and discusses new ways to mitigate changing threats against today’s networks.

*Index Terms*—Cisco Routers, Mitigation Techniques, Network Attacks, Security Threats

## I. INTRODUCTION

NETWORK administrators face many threats from both inside and outside the walls of their infrastructure. This paper discusses the risks that everyone faces along with ways to mitigate the exposure and resulting damage from such an attack. It will also focus on new devices being produced to provide increased security. Despite their slipping market share in router sales to Juniper, Cisco remains the largest provider of Routers, which are used to provide the backbone for the majority of companies today [10]. Because of the large role Cisco routers play in the infrastructure of the internet and the nature of the protocols these routers use; it has placed a large target on them from hackers wanting to exploit these vulnerabilities.

TABLE 1

ROUTER VENDORS 2004 ESTIMATED REVENUE

	Revenue	Share of the Market
<b>Cisco</b>	\$1.78 bil	56.9%
<b>Juniper</b>	\$971 mil	31.0%
<b>Redback</b>	\$92 mil	2.9%
<b>Nortel</b>	\$57 mil	1.8%
<b>Fujitsu</b>	\$48 mil	1.5%
<b>Other</b>	\$182 mil	5.8%
<b>Total</b>	<b>\$3.13 bil</b>	<b>100.0%</b>

Estimated Worldwide revenue and market share for 2004

## II. THREATS

### A. Physical Threats

Physical Security is of initial concern with any network. The best designed network means nothing if the physical security is lacking. In the cable and phone industry for example, the router will typically be installed in a building called a head-end or central office, which houses all the electronics that supply video and data services to a city or service area. The facility that houses these routers should be secure at all times and be accessible only by authorized personnel. To provide accountability of access, the use of electronic swipe cards should be used which will log access into the building. Cameras to monitor the facility should also be implemented to be able to monitor live the entrances and exits of the building as well as the surrounding perimeter.

### B. Environmental Threats

Environmental threats need to be controlled as well. All network hardware should be protected from the elements at all times. A dependable and redundant system of air conditionings and humidity controls need to be implemented and monitored. If possible the use of a humidifier and dehumidifier should be used to keep a proper humidity levels as climate area and air conditioners can affect greatly the proper levels of humidity in this controlled environment. Routers and switches should be placed in an equipment rack with the proper spacing between devices to allow for proper airflow. Typically you will want to allow one “rack unit” or RU between the equipment within the rack. The use of antistatic devices should also be used when dealing with sensitive equipment. If possible, the use anti-static floor tiles should be installed in the facility. At minimum the use of

anti-static wrist bands or other similar devices should be used when working around equipment to discharge any potential buildup of static electricity. Lastly the environment should be monitored continuously by means of sensors located at multiple points within the equipment room or head-end. An alarm triggering a HI or LOW temperature parameter should be sent to a remote monitoring facility, emailed, text messaged, or paged to the proper personnel. As a backup plan, fans should be stored nearby for use in an emergency, as they could mean the difference between keeping equipment online and functioning and being destroyed by the heat if a failure was to occur.

### C. Electrical Threats

Electrical Threat Mitigation should be focused on next and includes the following:

1. Install uninterrupted power supply (UPS) systems for mission-critical Cisco routing and switching devices
2. Install backup generator systems for mission-critical power supplies
3. Plan for and initiate regular UPS or generator testing and maintenance procedures based on the manufacturers suggested preventative maintenance schedule.
4. Use filtered power.
5. Install redundant power supplies on critical devices
6. Monitor and alarm power-related parameters at the supply and device levels. [11]

The installation of UPS's in the system will allow for the equipment to stay operational while the backup generator comes online. The UPS's also will filter the "dirty" generator power until utility power comes back online. UPS's and generators need to be inspected regularly as battery's can degrade over time in both devices. Monthly inspections should be performed on generators to check for such things as proper fuel levels, battery health, and radiator health and should be turned on and run for a period of time. If the generator has to be located close the equipment facility, care needs to be given to mitigate the vibration which could adversely affect the equipment.

Not all Cisco routing and switching gear come with dual power supplies. The low end routers, such as the 2600 line, do not include dual power for the sake of cost and size. Keeping whole spares of this type of equipment that does not support redundant power is a good practice. Low end routers such as these are not, and should not be used to serve any type of mission critical functions. Service providers who are getting into the market of voice over IP (VOIP) are required to use full redundancy for all gear associated in providing VOIP services to be able to be considered as a life line provider.

### D. Maintenance Threats

Regular maintenance should be performed on all gear in a timely manner. Some Cisco gear has devices such as fan trays and air screens that need to be inspected and/or replaced on a regular interval. Moving parts in any system are going to be the weakest link, so spare parts such as power supplies and fan trays should be stocked and clearly labeled for quick use in an emergency

## III. ANATOMY OF AN ATTACK

In its simplest form, an attack is categorized as the interruption, interception, modification, or fabrication of data from a valid source to its intended destination.

1. Interruption – An asset of the system is destroyed or becomes unavailable
2. Interception – An unauthorized party gains access to an asset
3. Modification – An unauthorized party gains access to and tampers with an asset
4. Fabrication – An unauthorized party inserts counterfeit objects into the system [14]

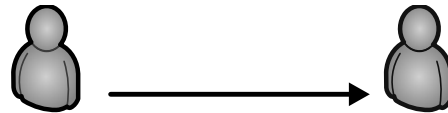


Fig. 1. Normal traffic flow pattern from source to destination

- a) *Normal flow* – Under normal conditions traffic should pass unobstructed from source to destination as in figure 1. A source of data is sending that data to an intended destination and that destination is receiving this data unobstructed and without it being compromised in any way, and in a perfect world this would be always be the case.

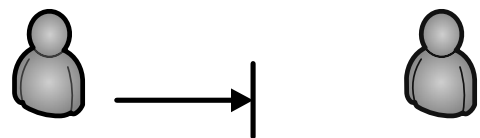


Fig. 2. Traffic interruption from source to destination by an attack

- b) *Interruption* – The first type of attack and among the simplest would be total packet flow interruption. This category can includes lots of different types of network attacks such as physical, discussed previously, which could be carried out by a person physically turning off the router or otherwise disabling it. The interruption of service may also be caused by an intruder gaining unrestricted access by means of telnet or some type of out of band management and commanding the routers interfaces to shut down thereby interrupting traffic. A Denial of Service (DoS) attack is an example of an attack where its purpose is the interruption of information.

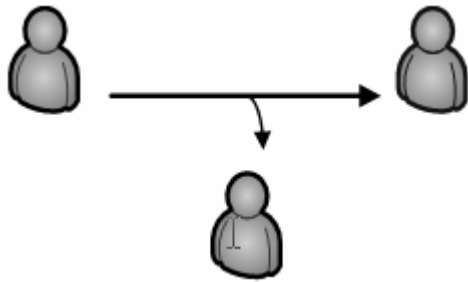


Fig. 3. Interception of traffic flow from source to destination by an unauthorized third party.

- c) *Interception* - A common type of attack, this attack is performed by snooping on network traffic to try to obtain data such as passwords, credit card numbers, or other types of sensitive information that may be transmitted in clear text. A Man in the Middle attack is an example of this category. The industry has developed many ways to try to protecting the hijacking of information in this way. Encryption means such as SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text. The use of “strong” encryption is always preferable since even though the text is encrypted the intruder does have the ability to capture and save this information and try to decrypt it passively. Some encryption methods are more easily broken than others so as the data being sent becomes more sensitive in nature, more care will need to be taken to protect that data from this type of intrusion.

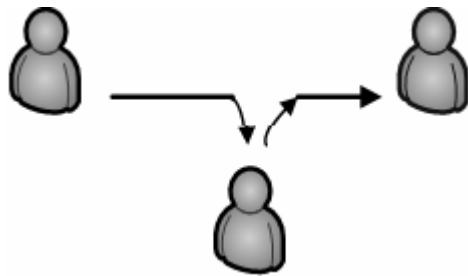


Fig. 4. Modification of traffic flow from source to destination by an unauthorized third party.

- d) *Modification* – Port Redirection would be a way for this type of attack to occur. In this case an attacker has been able to force traffic to flow from source to destination undetected through a 3<sup>rd</sup> party host to be able to modify or falsify data as it passes through. If done properly and if no detection methods are in place both the source and destination will have no way of knowing the traffic is being altered. An intruder performing this kind of attack could take incoming data from the source and attach viruses or other malicious code and send it along its way undetected to the destination. Mitigation techniques for this type of attack could be the introduction of

intrusion detection systems (IDS) which could look for different signatures which represent an attack. In the case of this example, the IDS may spot an unusual spike in latency for data to reach the destination. This increase in time would be from the intruder redirecting traffic and then altering traffic.

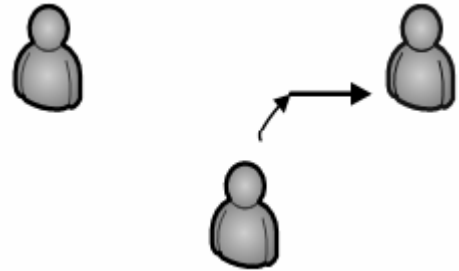


Fig. 5. Fabrication of traffic flow from unauthorized third party to destination. Third party is posing as a trusted source of information

- e) *Fabrication* – Much like Modification, Fabrication incorporates a 3<sup>rd</sup> party host sending data to the original destination of traffic. In this case the 3<sup>rd</sup> party could be spoofing the credentials of the original source thereby appearing to the end destination to be a valid and trusted source of information. This would be a more intrusive way to perform an attack if someone is monitoring the original source. In this case the original source is no longer sending or receiving traffic and may raise suspicions.

#### IV. TYPES OF NETWORK ATTACKS

Attacks on your network will come in all shapes and sizes. Before discussing the configuration changes that can help reduce the likelihood of being attacked or at least soften the blow of a successful attack, its best to dissect what type of network attacks exist.

##### A. Packet Sniffer

A “packet sniffer” is a network analysis tool that can display, record and analyze streams of packets from a network [15]. Several of the most popular sniffer programs include Ethereal (<http://www.ethereal.com>) which can not only sniff live network traffic but can capture the data for later analysis and decryption. Another packet sniffer program is Snort, (<http://www.snort.org>) which has basically the same functions as does Ethereal, and has a companion program for wireless networks; Air-Snort. Airtsnort.org describes its utility as “an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods”. A 3<sup>rd</sup> program worth mentioning is Cain and Abel (<http://www.oxid.it/cain.html>). This program can be considered the Swiss Army knife of utilities because it can perform a whole host of things. Not only will the program act as a packet sniffer but can perform dictionary and brute force attacks on different types of encryption, such as Cisco type 7

passwords, MD5 hash, and Cisco VPN passwords. These utilities in the hands of malicious parties can be dangerous for several reasons. Some common network protocols such as Telnet, FTP, SNMP and the popular E-mail protocol, Post Office Protocol (POP) are sent in clear text from source to destination. If an intruder intercepts the flow of this type of unencrypted data, then an attacker could become in possession of sensitive information.

It's best to mitigate the attack of these protocols by use of devices such as firewalls, strong encryption, and router IP access lists to thwart such an easy attack. Even with encrypted content, the packet sniffer can record content and be passively attacked "offline". The use of strong encryption techniques is encouraged for sensitive information. Another potential risk is users instinctively like to use the same passwords between different applications. If the packet sniffer picks up passwords in clear text, the attacker can use these passwords to try to gain access to other, more potentially sensitive applications. The use of strong authentication such as one-time passwords (OTP) provides a dual factor authentication. It requires something the user knows with something the user has. In this case the user can have a pin number that has to be entered along with a generated password from a token card. If the password is intercepted during transit, the password would be rendered useless within 30 seconds to 1 minute. This is a great way to mitigate such an unnecessary risk.

### B. Password Attacks

As mentioned earlier, password cracking is a feature of some packet sniffer programs. This allows an attacker to use such methods as brute force, or dictionary attacks to gain access to sensitive systems such as routers, switches, and network servers. In a dictionary attack, a use of a list of common words is used to try to gain access. The inherent nature of humans is to use passwords that are easily remembered. A dictionary attack exploits this type of vulnerability by using common dictionary words [4]. The brute force method is different in its method by the use of more random patters of numbers and characters to try to crack a password or hash. The time it takes to gain entry into a system by brute force can be considerable. The use of one-time passwords is an easy way to help protect from these types of attacks [5]. If this cannot be implemented then other measures such as disabling accounts or providing notifications after a certain number of failed attempts is desirable. This implementation will limit the number of times a password attack can be administered. The use of "strong" passwords are now being required by some major ISP's for their email systems to protect against these types of attacks. The same should be used in any organization that cannot implement OTP's. Password aging is another mitigation technique that can be implemented to force users to change passwords every so many days. Password aging should not be used as a stand alone mechanism, but as another layer of protection in a more

comprehensive security policy

### C. Denial of Service

Denial of Service and Distributed Denial of Service attacks (DoS, DDoS) are very popular types of attacks, not to mention very affective. In the case of a denial of service attack, the attacker is not necessarily trying to gain access to a protected system but his main objective is to deny others from that resource, for example a router, or web site. This is usually accomplished by use of an influx of bogus packets. In this type of attack the source of the attack will bombard the target with bogus IP information to tie up resources at the destination. The attacker will send packets with a spoofed or fake source destination, so when the routers respond back with an acknowledgement to the received packet the router will have an open connection while it waits for a response back from the fake source. The router will become flooded with these bogus incoming packets, keeping open ports tied up and causing utilization of the router to increase to the point of bring the router down and denying service to anyone else. This kind of attack is known as a SYN flood, and it sends a flood of TCP/SYN packets to a target router. These bogus TCP/SYN packets are handled like an ordinary connection request, causing the router or server to create a half-open connection, by sending back a TCP/SYN-ACK packet, and waiting for an TCP/ACK packet in response from the sender address. Because the source IP address is a spoofed or forged address the response is never received by the target router or server, eventually causing the resources of the device to saturate to the point where it becomes unusable [7] An even more severe type of DoS attack is the distributed denial of service attack. This new type of attack began to evolve in 2000. A DDoS attack uses resources from multiple systems using agent software that is controlled from a master system. This lets more packets be transmitted to the DoS's target [13] Since the packets being sent are packets that are typically allowed into a router, such as ICMP and TCP packets, mitigating these types of attacks can be difficult. Proper configuration of network routers and firewalls can help reduce the risk to this type of attack if the configuration includes RFC 2827 filtering. If the attackers cannot mask the source of their identities it may deter them from attacking in the first place [9]

### D. Man in the Middle Attacks

Resource [8]-[9], [15] describes the use the Man-in-the middle attack or MITM, as a way to gain access to the internal network resources, traffic analysis to drive information about the network, denial of service, corruption of transmitted data and the introduction of new information into the network sessions. To mitigate the effectiveness of this type of attack, strong encryption should be used. The MITM will be able to only see ciphered data instead of clear text data if the uses of such things as VPN's are used. One method of securing data

from host to a router in a cable based ISP is the introduction of Baseline Privacy Plus (BPI+)[18]. A new addition to the cable broadband industry is the use of off the shelf cable modems to supply a VPN type of solution at layer 2. It negates the need and overhead of VPN gear. A remote home user can use a cable modem which is configured to only communicate at layer 2 to another cable modem within the same ISP. An aggregation router back at the ISP's office is needed to bridge the traffic from the two cable modems. Since cable broadband is a shared medium, the use of BPI+ encryption is also used to protect against prying eyes and is HIPPA compliant.

#### E. *Trojans Viruses and Worms*

Other attack methods that can wreak havoc on an ISP are Trojan's viruses and worms. A virus for example, propagates throughout a network through the spread of email, graphic files, word documents, and spreadsheets [13] A virus cannot replicate on its own and requires users to pass the virus on to other unsuspecting users.

A worm is like a virus whereas it can propagate through a network. Unlike a virus, worms are stand alone programs, can replicate by themselves and do not require a host graphic file, or spread sheet to be transmitted [3]. Worms can use email systems to spread onto other networks by usually using an infected host's email address book to send copies of itself with flashy subject titles and email attachments to trick other parties into opening them. This can create a denial of service attack by increasing bandwidth usage as it replicates and can hog storage capacity on email servers. ISP's are increasingly offering its users free anti-virus and spam protection to thwart the outbreak of this kind of attack. It's in the ISP's best self interest to protect its network not only from the head end but by pushing out the protection to the networks edge (cable modems). Examples of popular worms include Nimda, CodeRed, and Slammer.

Trojan's are an attack mechanism that is disguised as a legitimate program [2]. For example, the user could download what looks to be a harmless game, when in fact the program is a harmful Trojan that is in the background emailing copies of itself to other systems as an attachment, thus potentially creating a form of DoS.

#### F. *Operator Error*

Lastly it must be stressed that in order to protect against these types of attacks, operator error needs to be mitigated as much as possible. Careful planning and thoughtful discussion with peers of significant router configuration changes need to be addressed as this could allow holes to open up in the protection the router has against these types of threats. One wrong keystroke could render access lists (ACL's) and other protection mechanisms useless, and open you to the attacks mentioned above. If multiple users must log into the router for different reasons, make sure that they are given just the

level of access necessary to complete their tasks. Network administrators need to have different rights than a tech who may need to check to make sure a device is online. Allowing unrestricted access will increase the likely hood of an unauthorized configuration change and unplanned downtime. Back ups of configuration files need to be saved after every change. If an attacker does gain access and wipes out the configuration, a backup close at hand will restore service quickly to allow for the investigation and post mortem phase to begin.

## V. ROUTER CONFIGURATION BEST PRACTICES

### A. *Cisco Router Introduction*

Cisco routers straight out of the box are set to pre-configure themselves with certain functions enabled or disabled that they deem critical features. An example of a feature that is by default turned off is "ip-http server". This is an unnecessary feature for the basic operation of the router and with some IOS versions easily exploited by hackers. For users who feel like the activation of this feature is worth the risk, enabling the feature is just a few key strokes away. What may be tricky is that some features disabled or enabled by default are sometimes not explicitly listed as so when displaying the configuration which means some due diligence is required on the operator's part in knowing the specific's of the particular IOS being utilized. It's always best to try to standardize the use of certain software releases throughout the organization for continuity sake. The use of mismatched IOS code of varying revisions can each contain its own unique vulnerabilities and the complexity of protecting the network compounds itself with this unnecessary risk When a vulnerability is discovered its best practice to push this IOS down to all routers as soon as possible to mitigate the risk. This next section will dig deeper into the configuration of key router configuration that can provide a baseline level of security. Because the application and implementation requirements of routers into a network are virtually limitless, this is only a recommendation, and may not be suitable for all applications.

### B. *Cisco Router Configuration Examples*

When fully booted the router will supply you a prompt of "Router>". A typical default configuration will appear similar to the following:

```
*****BEGIN*****
Router#sho run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```

!
hostname Router
!
!
ip subnet-zero
!
!
!
controller T1 1/0
!
!
!
interface FastEthernet0/0
no ip address
no ip directed-broadcast
shutdown
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
shutdown
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

Router#
*****END*****

```

For sake of simplicity, we will tackle the configuration from top to bottom. One of the first things that is suggested is to turn on the feature of password encryption. This feature is off by default. As passwords are set on the router, they are left in clear text. A hacker who is snooping a telnet session can easily spot the passwords as they travel in clear text. Once this feature is enabled all passwords configured will immediately be encrypted. Configuration of this command is shown below:

```

BrianF>en
Password:
BrianF#config t
Enter configuration commands, one per line. End with
CNTL/Z.
BrianF(config)#service password-encryption ?
<cr>
BrianF(config)#service password-encryption
BrianF(config)#^Z

```

The next phase in the process is to now add some basic passwords to the router. We will now add an enable password for the router as well as an enable secret password. The final listing of the configuration at the end of this section will show that the clear text enabled password entered has been encrypted. The enable secret password is encrypted automatically with MD5 hash, and is supposedly uncrackable.

```

BrianF(config)#enable password cisco1
BrianF(config)#enable secret cisco2

```

At this time it is also advisable to add a password to the console and vty interfaces. By default the router will not allow incoming connections via telnet until there is a password on the interface.

By default “no ip http server” is enabled and it is not advisable to turn this on, unless there is a strong need. If the feature was to be turned on via the “ip http server” global command, users would be able to connect to port 80 of your router and begin web based attacks. Figure 5 shows what users would see when trying to access the router via the web. At this point your router is open to attacks and once in, can have web based configuration capabilities.



Fig 5. Screen shot of web login interface with ip-http service command enabled

## Cisco Systems

### Accessing Cisco 2621 "BrianF"

[Telnet](#) - to the router.

[Show interfaces](#) - display the status of the interfaces.

[Show diagnostic log](#) - display the diagnostic log

[Monitor the router](#) - HTML access to the command line interface at level [0](#), [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#), [13](#), [14](#), [15](#)

[Connectivity test](#) - ping the nameserver.

[Show tech-support](#) - display information commonly needed by tech support.

[QoS Device Manager](#) - Configure and monitor QoS through the web interface.

#### Help resources

1. [CCO at www.cisco.com](#) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](#) - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. [cs.html@cisco.com](#) - e-mail the HTML interface development group.

Fig 6. Screen shot of router web based interface after successful login. From here user is able to make configuration changes.

Another router feature worth considering is the “exec-timeout” command on the console and vty interfaces. Terminals that are logged on to the router will be forced to time out their session and need to sign back on, to regain access to the router. It will also ensure that the maximum number of vty sessions do not stay tied up, thus causing an inability to access via telnet. The use of out of band management (OOB) would be a way to mitigate the chance of the device being remotely inaccessible. The following shows the configuration file with some of the configuration changes mentioned.

```
*****BEGIN*****
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname BrianF
!
enable secret 5 $1$vNUJ$jwLX5fVsRmJnxAYEbydfs.
enable password 7 03075218050070
!
ip subnet-zero
!
!
!
controller T1 1/0
!
!
!
interface FastEthernet0/0
ip address 10.10.10.10 255.255.255.0
no ip directed-broadcast
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
shutdown
!
```

```
ip classless
no ip http server
!
!
!
line con 0
exec-timeout 0 0
password 7 151104021725272179
login
transport input none
line aux 0
line vty 0 4
password 7 0012071F55
login
transport input telnet
!
end
*****END*****
```

Other notable features worth disabling unless there is a specific need to have then enabled are:

- “no ip bootp server” - which disables the routers ability to act as a bootp server which could open it up to attacks.
- “no cdp run” – command can be placed on a global as well as on an interface level to stop important and possibly unwanted router information from being transmitted to other Cisco routers on the network.
- ”no ftp-server write-enable” command should be used to turn off the routers ability to act as a FTP server which could allow users to read/write files to the directory of the router. In IOS release 12.3 this feature is now disabled by default.
- “no ip finger” command can be used to block other users on the network from finding out who is logged into the router, finding out what processes are running on the router, the line number and other information.

Access lists are also important to the security of any router. The use of access lists controls flow in and out of your network routers based on the source and destination IP traffic. The proper use of access lists can mitigate many attacks previously discussed. Access lists on a granular scale are beyond the scope of this paper however a basic access list configuration may look similar to this:

```
access-list 10 permit 10.10.10.11
access-list 10 deny 10.10.10.15
access-list 11 permit 10.10.10.11
no cdp run
!
snmp-server engineID local 000000090200003080C45DE0
snmp-server community readonly RO 10
snmp-server community readwrite RW 11
snmp-server enable traps tty
```

From this example a simple access list is setup defining what traffic is to be permitted and denied. You can this take the access list created and use that for example to control the use of SNMP traffic. In this example the only user allowed to use SNMP is 10.10.10.11. This user has the ability to read and write to this router via the SNMP agent. All other traffic will be denied access. Access lists are extremely powerful and a network administrator should always have some degree of access list in place.

## VI. TECHNOLOGICAL CONVERGENCE

There is a shift in the industry toward convergence of different technologies in the same platform for ease of operation and increased usability. Cisco for example has just released a far superior predecessor to its widely popular 2600 platform which was used to provide the examples above, the 2800 ISR. This integrated services router looks to included increased security and functionality including intrusion detection and prevention, VPN, and Firewall support including a host of others. With this new series of routers you can use the SDM (Security Device Manager) which is an easy to use GUI to easily navigate and administer the security features. Now with just a click of the mouse the router will automatically configure the router to adhere to best practice configuration, create and apply ACL's and setup the firewall features. Cisco leads the industry with the first routers to offer IPS functionality. Cisco IOS IPS is an in-line, deep-packet-inspection-based solution that helps Cisco IOS Software to effectively mitigate network attacks. [20]

## VII. CONCLUSION

In today's world, security risks are prevalent and due care and due diligence are needed. Network administrators need to be mindful of all the threats that exist and be able to combat those with skillfully designed network architectures and proper configurations to their routing, switching and network equipment. With the move to an IP platform carrying not just data but voice and video as well, great care will need to be given to having the proper equipment, configuration, and design to ensure a safe and secure network.

## REFERENCES

Wikipedia articles are licensed under the <http://www.gnu.org/copyleft/fdl.html> GNU Free Documentation License:

- [1][http://en.wikipedia.org/wiki/Computer\\_virus](http://en.wikipedia.org/wiki/Computer_virus)
- [2][http://en.wikipedia.org/wiki/Trojan\\_horse\\_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))
- [3] [http://en.wikipedia.org/wiki/Computer\\_worm](http://en.wikipedia.org/wiki/Computer_worm)
- [4] [http://en.wikipedia.org/wiki/Dictionary\\_attack](http://en.wikipedia.org/wiki/Dictionary_attack)
- [5][http://en.wikipedia.org/wiki/Brute\\_force\\_attack](http://en.wikipedia.org/wiki/Brute_force_attack)
- [6] [http://en.wikipedia.org/wiki/Password\\_cracking](http://en.wikipedia.org/wiki/Password_cracking)
- [7] [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
- [8][http://en.wikipedia.org/wiki/Man\\_in\\_the\\_middle\\_attack](http://en.wikipedia.org/wiki/Man_in_the_middle_attack)
- [9] J. Roland, CCSP Self-Study: Securing Cisco IOS Networks, Indianapolis, IN: Cisco Press, 2004, ch. 1.
- [10] A. Senia "IP Evangelist" America's Network, June 2005, pp. 5-6
- [11] J. Roland, CCSP Self-Study: Securing Cisco IOS Networks, Indianapolis, IN: Cisco Press, 2004, ch. 2.
- [12] J. Roland, CCSP Self-Study: Securing Cisco IOS Networks, Indianapolis, IN: Cisco Press, 2004, ch. 4.
- [13] Cisco Systems et al. Internetworking Technologies Handbook 4<sup>th</sup> edition, Indianapolis, IN: Cisco Press, 2004, pp 794-805
- [14] Carnegie Mellon "A Taxonomy of Computer and Network Attacks" <http://www.cert.org/research/JHThesis/Chapter6.html>
- [15] M.E. Whitman, Ph.D. and H.J. Mattord, M.B.A, Management of Information Security, Boston, MA: Thomson Course Technology, 2004, ch 9.
- [16] N. Mavrakis, "Vulnerabilities of ISP's" *IEEE Potentials* vol. 22. issue 4, pp 9-15, OCT-NOV 2003
- [17] C. M. Akujuobi and M.N. Sadiku "The present and future of broadband communications" *IEEE Potentials* vol 22, no 4, pp 12-16, OCT-NOV 2005
- [18] S. Green and K. Ozawa "BPI+ MIB Update" in Proc. IETF IPCDN Working Group, 2000, pp 1-14 <http://www3.ietf.org/proceedings/00dec/slides/IPCDN-2/sld001.htm>
- [19] P. Godwin IETF Journal vol 1 issue 1, 2005 pp1-28
- [20] [http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdccont\\_0900aecd80169b0a.pdf](http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdccont_0900aecd80169b0a.pdf) P.12