



## ***Cisco Router/Switch Hardening***

*Rocky Mountain Cisco Users Group  
March 12/13, 2003*



***William H. Gilmore | Scott R. Hogg***  
***International Network Services***

*T h e   k n o w l e d g e   b e h i n d   t h e   n e t w o r k ®*



## Agenda

- ◆ **Introductions**
- ◆ **First Half**
  - *What and why*
  - *Methodology*
  - *Booting & Banners*
  - *Keeping Time and Logging*
  - *Services Need & Not Needed*
  - *Interface Hardening*
  - *ACL's-o-plenty*
- ◆ **Break**
- ◆ **Second Half**
  - *Cisco IOS Firewall*
  - *SNMP Vulnerabilities*
  - *AAA*
  - *Securing Routers/Switches*
  - *Non-Cisco Security Tools*
- ◆ **Questions & Answers**

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



This presentation builds upon past Rocky Mountain CUG presentations

Kevin Parsons – January 2002

Trent Hein and Ned McClain – July 2002

Out of Scope:

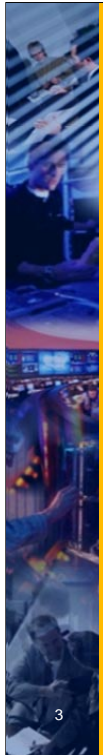
Firewalls (e.g. PIX)

Application Security

IPSec, VPNs


Covering Router IOS commands

Many other commands are in Cat OS and Cat IOS




## Router/Switch Hardening

- ◆ **What is hardening?**
  - *Controlling Access*
  - *Eliminating undesired traffic*
  - *Minimizing susceptibility to attacks*
  
- ◆ **Why do I need it?**
  - *Control who can access what when*
  - *Optimize device reliability and efficiency*
  - *Eliminate the possibility of many well known attacks to improperly configured devices*
  - *Minimize the effectiveness of unpreventable attacks (DDOS)*




www.ins.com  
The knowledge behind the network.®



Routers store the roadmap of a company's network, both internally and where they connect to the internet. Consequently, it is extremely important that routers run reliably and efficiently. Most routers within companies are located in their internal network. Their security configurations are usually minimal requiring a set of passwords for remote access and a simple read-only SNMP string. These settings are often adequate as the users of internal networks are bound by company security policies that dissuade users from attempting any malicious action.


Border routers do not share this same relatively secure environment. By definition, they are the router(s) that sits on the border between a company and the Internet. This makes them susceptible to all forms of attacks. Consequently, an improperly secured border router can easily be removed from service through even the simplest of attacks.

One has only to look back to February, 2002 to be reminded of just how vulnerable equipment can be to an attack. CERT® released Advisory CA-2002-03 warning of multiple vulnerabilities in almost all vendors implementation of Simple Network Management Protocol (SNMP). Shortly thereafter, companies, including telecommunications carriers, were attacked resulting in communication slow downs and outages. These attacks could have easily been avoided through following accepted security practices that had long been in existence prior to February, 2002.




## Methodology

- ◆ Provide password protection
- ◆ Configure privilege levels
- ◆ Limit remote access
- ◆ Limit local access
- ◆ Display login banner
- ◆ Configure SNMP
- ◆ Configure logging and NTP
- ◆ Provide other protection mechanisms
- ◆ Provide anti-spoofing
- ◆ Mitigate Denial of Service attacks
- ◆ Verify the configuration



[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*

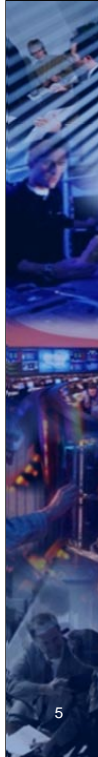


The following steps, identified in an article titled “Building Bastion Routers Using Cisco IOS”<sup>[1]</sup> are recommended when attempting to provide an acceptable level of security for WAN routers:

<sup>[1]</sup> <http://www.atomicgears.com/papers/bastionios.html>

As you attempt to secure your network. This methodology is a good way to start. Our presentation covers these areas though our order may vary.

Protection mechanisms for dynamic routing protocols.

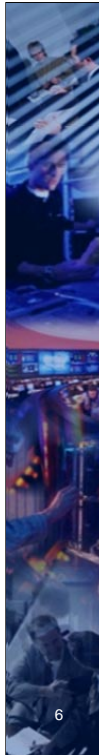


## Methodology

- ◆ **Additionally, one should include the following in their methodology.**
  - *Remove all services not needed*
  - *Enable strong passwords on all interfaces*
  - *Limit management capabilities*
- ◆ **Don't take anything for granted**
  - *Audit yourself before someone else does*

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®





## Boot ?


**Let's start at the beginning**

- ◆ **Default behavior**  

```
boot flash  
boot rom
```
- ◆ **Explicitly define which software image to be run**  

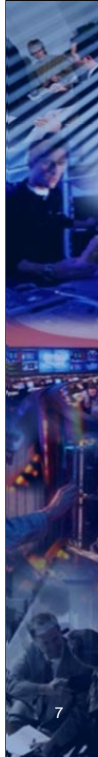
```
boot system flash c3640-js-mz.122-10a.bin  
boot system rom
```

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



6

The default behavior of IOS is to load the first image that it finds located in flash. If that image cannot be loaded successfully or if an image doesn't exist, then it boots from ROM. If a router is compromised, either physically or through a remote connection, it is possible that a different file could be placed in the flash that would load a "rogue" version of IOS on the router. By specifying the specific file to be loaded, one can minimize the possibility of a problem. Not that if you do explicitly define a flash file or even hardcode a "boot flash" command without a file name, the router will not attempt to boot from ROM in the event of a problem. This could render the router useless to remote remediation. So, add the "boot rom" statement to maximize a router's ability to be administered remotely in the event of a problem.




## A Little Legalese Please!

- ◆ Your router is public domain unless you post No Trespassing Signs
  - ◆ If you cannot identify
    - *What occurred*
    - *Where*
    - *When*
- then legally... it didn't!



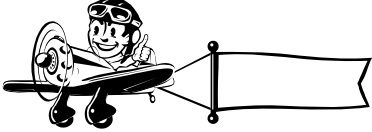
[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®





## Banners

- ◆ banner login
- ◆ banner motd ^C




```

banner motd ^C
*****
!! ONLY AUTHORIZED USERS ARE ALLOWED TO LOGON UNDER PENALTY
OF LAW !!
This is a private computer network and may be used only by
direct permission of its owner(s). The owner(s) reserves the
right to monitor use of this network to ensure network
security and to respond to specific allegations of misuse.
Use of this network shall constitute consent to monitoring
for these and any other purposes. In addition, the owner(s)
reserves the right to consent to a valid law enforcement
request to search the network for evidence of a crime stored
within this network.
*****
^C

```

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



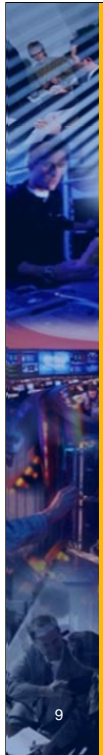
As a general practice banners should contain the following information and warnings:

- Only authorized personnel should gain access
- System logs are being maintained and could be used as evidence in criminal and/or civil court
- Unauthorized access is unlawful and is subject to civil and/or criminal penalties
- Be sure banners comply with corporate policies, so that the verbiage does not conflict with policies.
- Consider having banners reviewed by corporate legal counsel.

Things not to put in a banner

- Do not mention company name, physical device location.
- Never use the word 'welcome'.


Different banner messages may be used in different network locations. Border routers may use a message such as this one. Internal routers may include warnings regarding disciplinary actions in addition to or instead of criminal/civil actions.




## Time Synchronization

- ◆ Do you know what time it is?
- ◆ Use NTP to synchronize the routers clock to a high-level NTP Server
  - Stratum 1 GPS radio
  - Stratum 1 or 2 clock from ISP or NIST
  - Review <http://www.ntp.org> for NTP info
- ◆ Use NTP Authentication

```
clock timezone MST -7
ntp authentication-key 1 md5 <SECRETKEY>
ntp authenticate
ntp update calendar
ntp server 10.2.3.4
```



[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



David Mill's Network Time Synchronization Project Web Site  
<http://www.eecis.udel.edu/~mills/ntp.html>

Public Stratum 1 NTP Servers – National Institute of Standards  
<http://www.boulder.nist.gov/timefreq/service/time-servers.html>

If an interface does not need to receive NTP packets then use this interface command  
“ntp disable”

S

## Logging – Who’s the Hall Monitor?

- ◆ **Use service timestamps**  

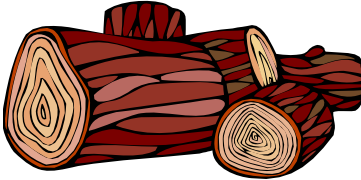
```
service timestamps debug datetime
service timestamps log datetime msec localtime
```
- ◆ **Configure syslog server(s)**  

```
logging 10.2.3.4
logging facility local7
```
- ◆ **Decide what to log**  


```
logging trap informational
logging console warnings
```
- ◆ **Decide where to log from**  

```
logging source-interface loopback0
```
- ◆ **Buffer those messages**  

```
logging buffered 4096
```



www.ins.com  
The knowledge behind the network.®



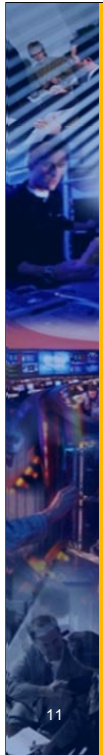
### NTP synchronization is vital to Logging and determining when security incidents occur

Here is an example of what should be entered into the routers. The IP address of the logging server is 10.2.3.4. For logs to be admissible as evidence in a court of law there must be verifiable time sources for logs. Hence NTP should be used to synchronize the times on routers to an accurate source. It is desirable to have logging to the informational (6) level for good granularity of events.

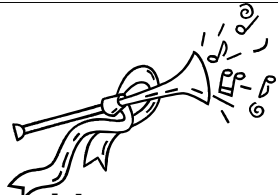
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122csum/csum1/122csfun/fsf013.htm#19650>

#### Error Message Logging Priorities and Corresponding Level Names/Numbers

Level	Arguments	Level	Description	Syslog Definition
emergencies		0	System unusable	LOG_EMERG
alerts		1	Immediate action needed	LOG_ALERT
critical		2	Critical conditions	LOG_CRIT
errors		3	Error conditions	LOG_ERR
warnings		4	Warning conditions	LOG_WARNING
notifications		5	Normal but significant condition	LOG_NOTICE
informational		6	Informational messages only	LOG_INFO
debugging		7	Debugging messages	LOG_DEBUG




## Tuning the IP stack



- ◆ **Nagle congestion control algorithm**  
*service nagle (See RFC 896)*
- ◆ **Limit embryonic TCP connections**  
*ip tcp synwait-time 10 (30 seconds default)*
- ◆ **Other special cases**  
*ip tcp window-size 2144 (RFC 1323)*  
  
*ip tcp selective-ack (See RFC 2018)*

[www.ins.com](http://www.ins.com)  
 The knowledge behind the network.®



Nagle – RFC 896 – Jan 1984

**service nagle**

The Nagle Algorithm prevents excessive bandwidth utilization by applications that send many small packets. It allows slight delays before sending individual small packets in order to combine them into a single larger packet.

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wccomm/html/\\_wccesdk\\_Nagle\\_Algorithm.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wccomm/html/_wccesdk_Nagle_Algorithm.asp)

Useful for really old hardware and really slow network links

To help limit the vulnerability to TCP SYN-Flood attacks, use the global configuration “ip tcp synwait-time” command to limit the seconds that the router spends waiting for the ACK before giving up on a half-open connection.

To set a period of time the Cisco IOS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** global configuration command. To restore the default time, use the **no** form of this command. **ONLY works on traffic originating from the router.**

**ip tcp synwait-time** seconds

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ae127.html#1001831](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ae127.html#1001831)

**ip tcp window-size 2144** - 2144 bytes default (RFC 1323 )

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a0080087d52.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d52.html)

TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round trip time. An aggressive sender could retransmit packets early, but such retransmitted segments might have already been successfully received.

The TCP selective acknowledgment mechanism helps overcome these limitations. The receiving TCP returns selective acknowledgment packets to the sender, informing the sender about data that has been received. The sender can then retransmit only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when multiple packets drop from a TCP window. There is no performance impact when the feature is enabled but not used.

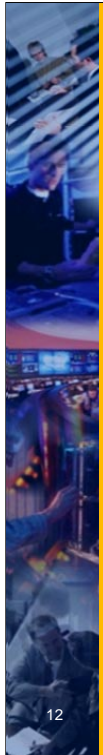
**ip tcp selective-ack**

This command becomes effective only on new TCP connections opened after the feature is enabled.

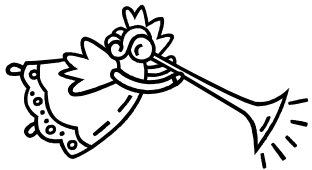
This feature must be disabled if you want TCP header compression. You might disable this feature if you have severe TCP problems.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1826/products\\_command\\_summary\\_chapter09186a00800d9c53.html#xtocid2738927](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800d9c53.html#xtocid2738927)




## Tuning the CPU



- ◆ **Guarantee CPU time for vital processes**  
*scheduler-interval 500 (500 milliseconds)*
- ◆ **More granular on Cisco 7200 & 7500 platforms**  
*scheduler allocate 500 100*  
*(500 microseconds per clock cycle on fast-packet switching)*  
*(100 microseconds per clock cycle on processes switching)*

12

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



The **scheduler interval** command allows low priority processes to be scheduled every 500 usec, thereby allowing some commands to be typed even if CPU usage is at 100%.

You can prevent or impede some Denial of Service attacks caused by very fast packet floods by changing the routers scheduling interval.

### **scheduler interval**

To control the maximum amount of time that can elapse without running system processes, use the scheduler interval global configuration command. To restore the default, use the no form of this command.

**scheduler interval** milliseconds

**no scheduler interval**

### **scheduler allocate**

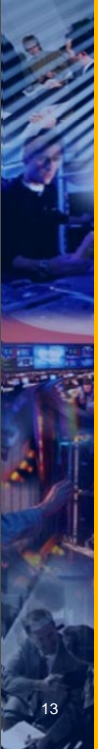
To guarantee CPU time for processes, use the scheduler allocate global configuration command on the Cisco 7200 series and Cisco 7500 series routers.

The **scheduler allocate** command guarantees CPU time for low priority processes by putting a maximum time allocated to fast-switching (3000 microseconds - usec) and process-switching (1000 usec) per network interrupt context.

To restore the default, use the no form of this command.

**scheduler allocate** interrupt-time process-time


**no scheduler allocate**



## Services - Needed

- ◆ `service password-encryption`
- ◆ `service tcp-keepalives-in`
- ◆ `service tcp-keepalives-out`
- ◆ `service timestamps debug datetime`
- ◆ `service timestamps log datetime localtime`

[www.ins.com](http://www.ins.com)  
 The knowledge behind the network.®



### **service password-encryption**

To encrypt passwords, use the `service password-encryption` command in global configuration mode. To restore the default, use the `no` form of this command.

#### **service password-encryption**

The TCP keepalive capability allows a router to detect when the host with which it is communicating experiences a system failure, even if data stops being transmitted (in either direction). This is most useful on incoming connections. For example, if a host failure occurs while talking to a printer, the router might never notice, because the printer does not generate any traffic in the opposite direction. If keepalives are enabled, they are sent once every minute on otherwise idle connections. If five minutes pass and no keepalives are detected, the connection is closed. The connection is also closed if the host replies to a keepalive packet with a reset packet. This will happen if the host crashes and comes back up again. To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the `service tcp-keepalives-in` global configuration command. To disable the keepalives, use the `no` form of this command.

#### **service tcp-keepalives-in**

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the `service tcp-keepalives-out` global configuration command. To disable the keepalives, use the `no` form of this command.


#### **service tcp-keepalives-out**

To configure the system to time-stamp debugging or logging messages, use one of the `service timestamps` global configuration commands. To disable this service, use the `no` form of this command.

**service timestamps** message-type [**uptime**]

**service timestamps** message-type **datetime** [**msec**] [**localtime**] [**show-timezone**]


**no service timestamps** type



## Services – Not Needed

- ◆ `no cdp run` *(be careful)*
- ◆ `no boot network` *(older command)*
- ◆ `no service config`
- ◆ `no ip source-route`
- ◆ `no service finger` *(older command)*
- ◆ `no ip finger`
- ◆ `no ip identd`
- ◆ `no service pad`
- ◆ `no service tcp-small-servers`
- ◆ `no service udp-small-servers`
- ◆ `no ip bootp server`
- ◆ `no snmp-server` *(more on this later)*
- ◆ `no tftp-server`

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



To CDP or not to CDP, that is the question! On border routers, it is unlikely that CDP is needed. So, turn it off globally using:

```
no cdp run
```

If the router is internal or if CDP is needed, then run the global CDP process; however, refer to the following interface section on how to enable/disable CDP on individual interfaces. Beware, some services such as the use of Cisco's VoIP phone implementation require CDP in order to operate properly.

To disable the automatic loading of configuration files from a network server turn off the service configuration. This service does not depend upon any type of authentication or confirmation regarding the validity of the data stream that it receives from the service. This makes this service potentially susceptible to compromising the configuration of the router.

```
no service config
```

To disable the finger service (RFC 742) from running on, and being forwarded by the router, enter the following global configuration command. The finger service can be exploited and should therefore be disabled.

```
no service finger
```

To not accept incoming/outgoing X.25 Packet Assembler/Disassembler (PAD) connections this global configuration command should be used. It is important to make sure this is disabled by default.

```
no service pad
```

To enable identification support, use the **ip identd** global configuration command in RFC931 and RFC1413:

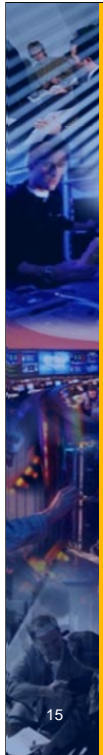
```
no ip identd
```

To protect against SYN-Flood attacks the following two global configuration commands should be entered into the configuration. These commands turn off echo and discard ports on the router. These help prevent against SYN-Flood attacks and UDP diagnostic port denial of service attacks on routers.

```
no service udp-small-servers
no service tcp-small-servers
```


Do not run the on-by-default bootp server. It is not needed so it should be disabled with the following global configuration command.


```
no ip bootp server
```



## Interface Hardening

- ◆ **no cdp enable**
- ◆ **ip accounting access-violation**
- ◆ **no ip directed-broadcast**
- ◆ **no ip redirects**
- ◆ **no ip unreachable**  
*no ip mask-reply*
- ◆ **no ip proxy-arp**
- ◆ **no mop enabled**
- ◆ **shutdown**





[www.ins.com](http://www.ins.com)  
 The knowledge behind the network.®

15

Disable Cisco Router Discovery Protocol (CDP) on the external interface(s) if it is not needed by entering the following interface configuration command.

no cdp enable

Enable ip accounting and have it log access-list violations to the system log.

ip accounting access-violation

Disable translation of directed to physical broadcasts on the same interface. This interface configuration command prevents against “smurf” attacks.

no ip directed-broadcast

Don’t allow redirect messages to pass through the router. ICMP redirects should be disabled with the following interface configuration command.

no ip redirects

Make it more difficult for someone to scan for valid IP addresses by turning off ip unreachables on all interfaces.

no ip unreachables

To prevent the Cisco IOS software from responding to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages

no ip mask-reply

Disable this if not needed on the router interface with the following interface configuration command. (RFC 1027)

no ip proxy-arp

Disable the Maintenance Operating Protocol (MOP) by applying “no mop enabled” to each interface.

no mop enabled

Shutdown the interface if it is not in use


W

## ACL - General

- ◆ **Basic**  
`access-list 1 permit 1.1.2.0 0.0.1.255`
- ◆ **Extended with remark**  
`access-list 100 remark telnet access list`  
`access-list 100 permit tcp host`  
`1.1.1.1 2.2.2.0 0.0.0.255 telnet`
- ◆ **Type-Code**  
`access-list 200 permit 0x0000 0x0d0d`
- ◆ **Named**  
`ip access-list standard allow-telnet`  
`remark machine from which telnet is accepted`  
`permit 1.1.1.1`  
`permit 2.2.2.2`

16

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



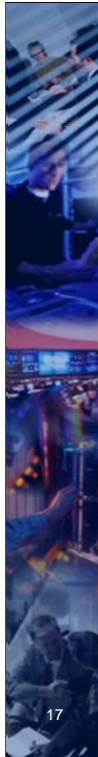
You should also mention how you can comment your ACLs.

Here is the reference:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ae127.html#40480](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ae127.html#40480)

ACLs:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ae127.html#1109098](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ae127.html#1109098)



## ACL – Time Based

```
access-list 100 remark Only allow IP traffic during  
open hours
```

```
access-list 100 permit ip any any time-range only-  
during-open-hours
```

```
!
```

```
time-range only-during-open-hours  
absolute start 00:00 01 January 2002  
periodic weekdays 7:30 to 18:30  
periodic Saturday 8:30 to 13:30  
periodic Sunday 8:30 to 18:30
```



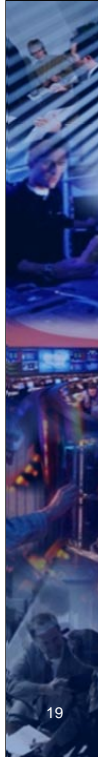
[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



## ACL – Lock & Key



```
interface ethernet0
 ip address 172.18.23.9 255.255.255.0
 ip access-group 101 in
 access-list 101 permit tcp any host 172.18.21.2 eq
 telnet
 access-list 101 dynamic mytestlist timeout 120 permit
 ip any any
 line vty 0
 login local
 autocommand access-enable timeout 5
```



## ACL – TCP Intercept

### ◆ Syn Flood Protection for Servers

### ◆ Two Modes

- *Watch* – Watches and terminates incomplete connections.
- *Intercept* – Attempts to complete connection with client on behalf of server. If successful, creates a connection to server. If unsuccessful, closes connection to client.

```
access-list 120 remark Web Servers
access-list 120 permit tcp any 1.1.1.0 0.0.0.255
ip tcp intercept list 120
ip tcp intercept mode watch
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept one-minute low 1500
ip tcp intercept one-minute high 6000
```

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



19

**TCP intercept is syn flood protection for servers.**

There are 2 modes Watch mode and Intercept mode.

**Watch mode** passively watches connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.

**Intercept mode** intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently.

#### Commands:

```
access-list access-list-number {deny | permit} tcp any destination destination-wildcard
ip tcp intercept list access-list-number
ip tcp intercept mode {intercept | watch}
```

By default, the software drops the oldest partial connection. Alternatively, you can configure the software to drop a random connection. To set the drop mode, perform the following task in global configuration mode:

```
ip tcp intercept drop-mode {oldest | random}
```

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset to the server. To change this value, perform the following task in global configuration mode:

```
ip tcp intercept watch-timeout seconds
```

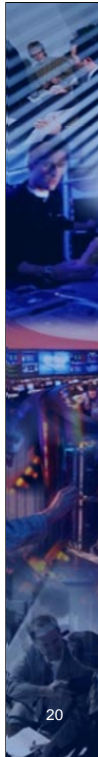
By default, the software waits for 5 seconds from receipt of a reset or FIN-exchange before it ceases to manage the connection. To change this value, perform the following task in global configuration mode:

```
ip tcp intercept finrst-timeout seconds
```

By default, the software still manages a connection for 24 hours after no activity. To change this value, perform the following task in global configuration mode:

```
ip tcp intercept connection-timeout seconds
```

Two factors determine when aggressive behavior begins and ends: total incomplete connections and connection requests during the last one-minute



## ACL – Reflexive

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group inboundfilters in
  ip access-group outboundfilters out
  !
  ip reflexive-list timeout 120
  !
  ip access-list extended outboundfilters
    permit tcp any any reflect tcptraffic
  !
  ip access-list extended inboundfilters
    permit bgp any any
    permit eigrp any any
    deny icmp any any
    evaluate tcptraffic
```

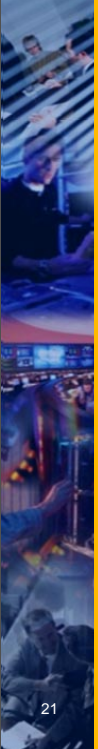


20

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



Cisco's early attempt at simulating stateful packet inspection.




## ACL – Reverse Path Forward

```


ip cef distributed
!
int eth0/1/1
  ip address 192.168.200.1 255.255.255.0
  ip verify unicast reverse-path 197
!
int eth0/1/2
  ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log

```



21

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



### Unicast RPF with ACLs and Logging Example

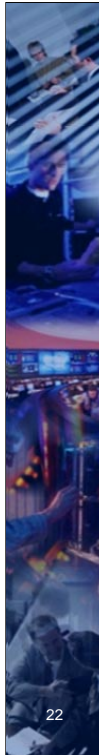
The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (logging option turned on for the ACL entry) to the log server.

```

Central# config t
Central(config)# ip cef
Central(config)# interface eth 0/0
Central(config-if)# ip verify unicast reverse-path
Central(config-if)# exit

```




## ACL – Where ICMP is Needed

- ◆ **ICMP is used to determine the MTU for a TCP connection.**

```
access-list 110 permit icmp any any packet-too-big
```
- ◆ **To allow outbound ICMP, use:**


```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any parameter-problem
access-list 102 permit icmp any any source-quench
access-list 102 deny icmp any any log
```
- ◆ **To allow outbound UNIX/Cisco Traceroute:**

```
access-list 102 permit udp any any range 33400 34400 log
```



22

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



Eliminating all ICMP will cause MTU determination to be conducted falsely and may lead to connection drops!

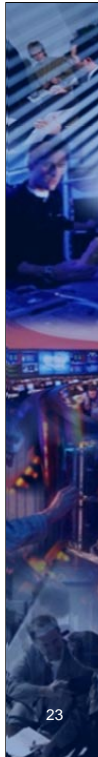
**Cisco traceroute starts at UDP port 33434 and then adds 3 to the port number for each test/hop**

Traceroute can be filtered thus limiting its usefulness

Traceroute's latency figures are not necessarily accurate

One can also limit the rate at which ICMP unreachable are sent from the router with the following command:

Router(config)# **ip icmp rate-limit unreachable [df] milliseconds**



## ACL - Turbo



### ◆ Turbo ACLs introduced in 12.1.5T for high-end Cisco routers

- Time taken to match the packet is fixed
- Latency of the packets is smaller and, more importantly, consistent
- Allows better network stability and more accurate transit times.

### ◆ Processes ACLs more efficiently

```
access-list compiled
show access-list compiled
```

23

www.ins.com  
The knowledge behind the network.®



### Turbo ACLs

Turbo ACLs were introduced in Cisco IOS Software Release 12.1.5.T and are found only on the 7200, 7500, and other high-end platforms. The turbo ACL feature is designed to process ACLs more efficiently in order to improve router performance.

Use the **access-list compiled** command for turbo ACLs. An example of a compiled ACL is shown below.

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

After defining the standard or extended ACL, use the **global configuration** command to compile.

*!-- Tells the router to compile.*

```
access-list compiled
```

### Interface Ethernet0/1

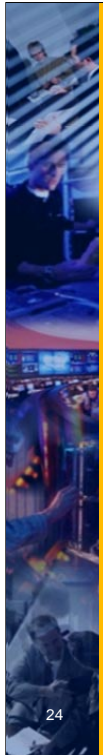
```
ip address 172.16.1.2 255.255.255.0
```

*!-- Applies to the interface.*

```
ip access-group 101 in
```


The **show access-list compiled** command shows statistics about the ACL.


[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ae127.html#80538](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ae127.html#80538)



## Limit Traffic To the Router

- ◆ **Limit traffic that can terminate at router**
  - *NTP*
  - *Telnet*
  - *SNMP*
  - *HTTP*
  - *TFTP*
- ◆ **Only allow traffic to the router that should terminate on the router**
- ◆ **Only allow traffic through the router that is sourced from or destined to known networks**





www.ins.com  
The knowledge behind the network.®

24

### Limit Traffic To and From Router

Traffic to and from the router should be limited to known traffic needed for management purposes. The following access lists limits ntp traffic both external and internal.

```
access-list 100 permit udp 12.xx.xx.0 0.0.1.255 host 12.xx.xx.1 eq ntp
access-list 100 permit udp host 12.xx.xx.1 12.xx.xx.0 0.0.1.255 eq ntp
access-list 100 permit udp host 128.138.140.44 host 12.xx.xx.162 eq ntp
access-list 100 permit udp host 12.xx.xx.162 host 128.138.140.44 eq ntp
access-list 100 permit udp host 132.163.4.103 host 12.xx.xx.162 eq ntp
access-list 100 permit udp host 12.xx.xx.162 host 132.163.4.103 eq ntp
access-list 100 permit udp host 192.43.244.18 host 12.xx.xx.162 eq ntp
access-list 100 permit udp host 12.xx.xx.162 host 192.43.244.18 eq ntp
```

The following access list allows the router to send syslog traffic to the internal syslog server.

```
access-list 100 permit udp host 12.xx.xx.1 host 12.xx.xx.138 eq syslog
```

The following access list is applied to the virtual terminal interfaces to limit telnet access to traffic that originates from within [Client].

```
access-list 1 permit 12.xx.xx.0 0.0.1.255
access-list 1 deny any
```

### [Client] Traffic

Apply the following access list to both the internal and external router interfaces to insure that traffic through the [Client] border router(s) is limited to source/destinations that are in use within [Client]. In the current case, these are the addresses used for Network Address Translation (NAT) on the PIX.

```
access-list 100 permit ip any 12.xx.xx.0 255.255.254.0
access-list 100 permit ip 12.xx.xx.0 255.255.254.0 any
```

## Limit Traffic Through the Router AKA - Anti-Spoofing Rules

- ◆ Anti-spoofing is used to prevent your router from transmitting data for address patterns that don't make sense!



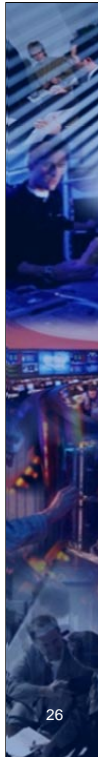
- *Inbound to address not within your network.*
- *Inbound from addresses that should be within your network*
- *Inbound from non-assigned addresses (Bogons)*
- *Outbound from RFC 1918 Private Addresses*
- *Outbound from addresses not within your network*

25

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



The point about anti-spoofing is to prevent people external to you sending you packets sourced from your addresses. It is also to prevent you from sending out packets not sourced from your own address space. Regardless, it is always good to filter in both directions. Performance is less of a concern now with fast-switching and CEF, but maintenance is still an issue. Keep in mind that ACLs can't do what a stateful firewall can do.



## Anti-spoofing ACL

```
! RFC 1918 private networks
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
! Historical Broadcast
access-list 100 deny ip host 0.0.0.0 any
! Loopback (IANA)
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
! unassigned address space
access-list 100 deny ip 128.0.0.0 0.255.255.255 any
! linklocal (IANA)
access-list 100 deny IP 169.254.0.0 0.0.255.255 any
! (191/8 emergency yet used)
access-list 100 deny ip 191.255.0.0 0.0.255.255 any
! Net root LV lab (IANA)
access-list 100 deny IP 192.0.0.0 0.0.0.255 any
! Example network (IANA)
access-list 100 deny IP 192.0.2.0 0.0.0.255 any
! ????
access-list 100 deny ip 223.255.255.0 0.0.0.255 any
! Multicast Addresses
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
! Reserved Class E
access-list 100 deny ip 240.0.0.0 15.255.255.255 any
! Explicit Deny
access-list 100 deny ip any any log
```

26

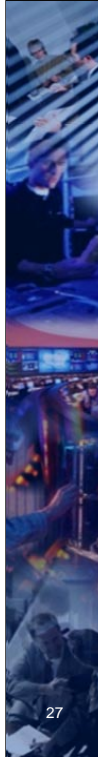
[www.ins.com](http://www.ins.com)

*The knowledge behind the network.®*



For one of the most comprehensive Anti-spoofing ACL, see Rob Thomas' SecureIOS Template and his Bogon list.

<http://www.cymru.com/Documents/secure-ios-template.html>



27

# Break


[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



S


## Cisco IOS Firewall

- ◆ Part of the Cisco Secure product family
- ◆ Security-specific option for Cisco IOS software
- ◆ Integrates robust firewall functionality and intrusion detection for every network perimeter
- ◆ Enriches existing Cisco IOS security capabilities
- ◆ Adds greater depth and flexibility to existing Cisco IOS security solutions



28

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



Who here has used the Cisco IOS Firewall feature set?

Cisco IOS Firewall Q & A – 12.0(5)T


[http://www.cisco.com/en/US/products/sw/secursw/ps1018/products\\_qanda\\_item09186a00800a3c74.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_qanda_item09186a00800a3c74.shtml)

Recent vulnerability in IOS firewall

[http://www.cisco.com/en/US/products/sw/secursw/ps1018/products\\_security\\_advisory09186a00800941ee.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_security_advisory09186a00800941ee.shtml)

This vulnerability is documented as Cisco Bug ID **CSCdv48261**.

IP protocol type is not checked by CBAC. This could allow a packet of different protocol type into the protected network.



## Cisco IOS Firewall - Info


### *Supported Hardware*

- ◆ Cisco 1700, 2600, 3600, 7100, 7200, 7500, and RSM

### *Supported Functionality*

<ul style="list-style-type: none"> <li>■ <i>Context-Based Access Control (CBAC)</i></li> <li>■ <i>Java blocking</i></li> <li>■ <i>Denial-of-service (DoS) detection and prevention</i></li> <li>■ <i>Real-time alerts</i></li> <li>■ <i>Audit trail</i></li> <li>■ <i>Authentication proxy (for dynamic, user-based authentication and authorization)</i></li> </ul>	<ul style="list-style-type: none"> <li>■ <i>Intrusion detection</i></li> <li>■ <i>Dynamic port mapping</i></li> <li>■ <i>Simple Mail Transfer Protocol (SMTP) attack detection and prevention</i></li> <li>■ <i>Configurable alerts and audit trail</i></li> <li>■ <i>IP fragmentation attack prevention</i></li> <li>■ <i>Microsoft-NetShow application support</i></li> </ul>
--	---

www.ins.com  
The knowledge behind the network.®

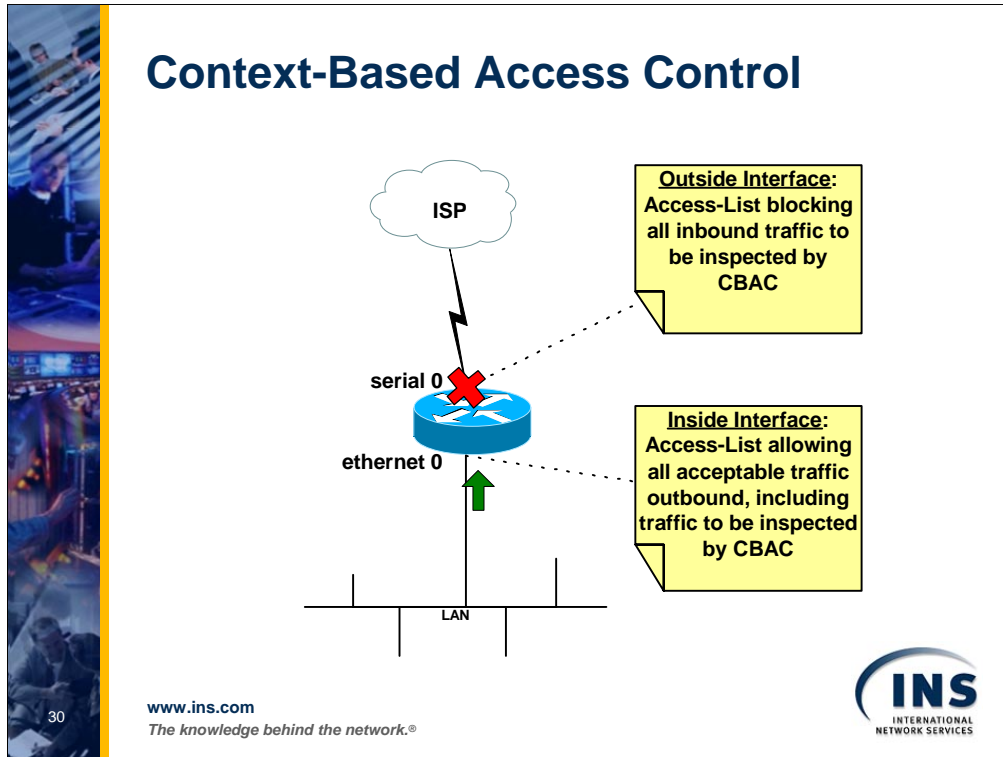


29

CBAC only supports TCP and UDP

Supported protocol-based inspection for the following:

- CU-SeeMe
- FTP
- H.323 (NetMeeting, ProShare)
- HTTP (Java blocking)
- Java
- Microsoft NetShow
- UNIX R-commands (such as rlogin, rexec, and rsh)
- RealAudio
- RPC (Sun RPC, not DCE RPC)
- Microsoft RPC/SMTP – but not ESMTP
- SQL \*Net
- StreamWorks
- TFTP
- VDOLive



An inbound IP access list (standard or extended) is applied to the internal interface. This access list permits all packets that you want to allow to exit the network, including packets you want to be inspected by CBAC.

An inbound extended IP access list is applied to the external interface. This access list denies any traffic to be inspected by CBAC. When CBAC is triggered with an outbound packet, CBAC creates a temporary opening in the inbound access list to permit only traffic that is part of a valid, existing session...

Order of packet processing when an outbound packet arrives at an interface:

1. The inbound ACL of the input interface is applied.
2. The NAT inbound is applied.
3. The NAT outbound is applied.
4. The outbound ACL of the output interface is applied.
5. **CBAC processing occurs.** (just before it leaves the router – permits the return traffic)
6. The IP Packet goes through the output interface.

**ip inspect name** *ruleset-name protocol [alert on/off] [audit-trail on/off] [timeout override-timeout]*

Length of time CBAC waits for a new TCP session to reach established state. Default: 30 seconds, Suggested: 15 seconds

South(config)# **ip inspect tcp synwait-time 15**

Length of time that CBAC continues to manage a TCP session after it has been closed down by a FIN exchange. Default: 5 seconds, Suggested: 1 second

South(config)# **ip inspect tcp finwait-time 1**

Length of time that CBAC continues to manage a TCP session with no activity. Default: 1 hour, Suggested: 30 minutes (1800 sec.)

South(config)# **ip inspect tcp idle-time 1800**

Length of time that CBAC continues to manage a UDP 'session' with no activity. Default: 30 seconds, Suggested 15 seconds

South(config)# **ip inspect udp idle-time 15**

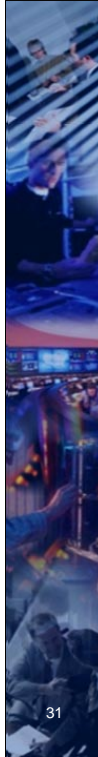
And

**ip inspect one-minute [high | low] <#>**

**ip inspect max-incomplete [high | low] <#>**

**ip inspect tcp max-incomplete host 50 block-time 0**

**ip inspect dns-timeout 5**



## IOS Firewall Example

```

interface Serial0/0
  ip access-group 116 in
  ip inspect myfw in
  ip auth-proxy mywebproxy
...
access-list 116 permit tcp any any eq www
access-list 116 permit tcp any any eq smtp
access-list 116 deny ip any any
...
ip inspect name myfw http timeout 3600
ip inspect name myfw smtp timeout 3600
...
ip auth-proxy name mywebproxy http
...
ip http authentication aaa
ip http server

```

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



31

This sample configuration initially blocks traffic from a host device on the internal network to all devices on the Internet until browser authentication is performed using authentication proxy. The access list passed down from the server (permit tcp|ip|icmp any any) adds dynamic entries post-authORIZATION to access list 116 that temporarily allow access from that device to the Internet.

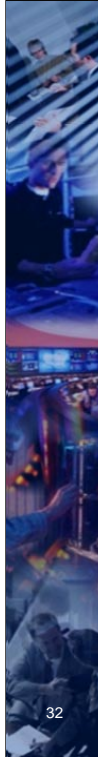
```

ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http

interface FastEthernet0/0
ip access-group 116 in
ip auth-proxy list_a

access-list 116 permit tcp host 10.31.1.47 host 10.31.1.150 eq www
access-list 116 deny tcp host 10.31.1.47 any
access-list 116 deny udp host 10.31.1.47 any
access-list 116 deny icmp host 10.31.1.47 any
access-list 116 permit tcp 10.31.1.0 0.0.0.255 any
access-list 116 permit udp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 171.68.118.0 0.0.0.255

```



# Simple Network Management Protocol

## ◆ SNMPv1

- Ubiquitous support
- Clear text Community Strings

## ◆ SNMPv2c

- Security the same as SNMPv1 – just a feature upgrade
- Hierarchical Network Management
- Get-bulk and Inform operators added
- New PDU format for traps introduced
- 64 bit counters (32 bit used for SNMPv1)

## ◆ SNMPv3

- Encrypted user-based authentication and data
- View-Based Access Control Model (VACM)

www.ins.com  
The knowledge behind the network.®



Source: <[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun\\_c/fcprt3/fcd301.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301.htm)>  
<http://netman.cit.buffalo.edu/FAQs/snmp-p1.faq> <http://netman.cit.buffalo.edu/FAQs/snmp-p2.faq>

All Cisco IOS Software releases to date include SNMPv1.  
Releases from Cisco IOS Software 11.2(6)F and later have SNMPv2C support.  
Releases from Cisco IOS Software 12.0(3)T and higher have SNMPv3 support.

RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.  
SNMPv2c (the "C" stands for "community") is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906.  
SNMPv2 Classic – uses the same clear-text community string as SNMPv1  
SNMPv2C support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

Added Informs, but still Community-based authentication  
INFORMs – SNMP v1 traps are unreliable – these are better – uses acknowledgement

SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273-2275.  
SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet.

View-Based Access Control Model (VACM)

V3 – MD5 or SHA community/authentication

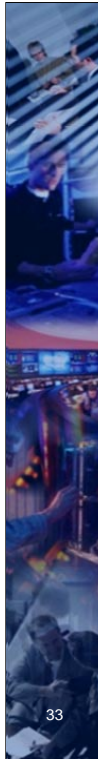
Different levels of access:

“noAuthNoPriv” – username/pass - User-Based Security Model (USM) – username/pass send in clear, no encryption

“authNoPriv” – HMAC-MD5 or HMAC-SHA, no encryption

“authPriv” – DES 56-bit encryption in addition to authentication based on DES-56

V1 uses clear text community strings - V2c encrypts the community – V3 encrypts the user password



## SNMP Vulnerabilities

- ◆ **Cert/CC SNMP Advisory**
  - *Issued Feb 12<sup>th</sup>, 2002 (CA-2002-03)*
- ◆ **SNMP implementations lack boundary checking and error handling which leads to buffer overflows**
- ◆ **Bounce attacks**
- ◆ **Known exploits exist and are publicized**
- ◆ **DOS attacks for routers, wireless APs, Windows, and printers**
- ◆ **Apply vendor patches promptly after testing**
- ◆ **Consider turning SNMP off where its not needed**
- ◆ **Control your security perimeter**

33

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



### CERT/CC SNMP Advisory

Issued Feb 12<sup>th</sup>, 2002

Identified multiple vulnerabilities

<http://www.cert.org/advisories/CA-2002-03.html>

### OUSPG PROTOS Project

Tested HTTP, WAP/WSP, LDAP and SNMP

Additional protocol testing will follow

### SNMP is huge target

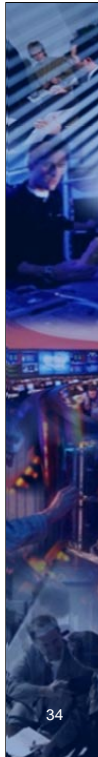
Nearly every device from every vendor could be affected

Many exploits are theoretically possible

A few exploits work now

More exploits will be developed

Phrack Volume Seven, Issue Fifty 7 of 16, 1997 - Network Management Protocol Insecurity: SNMPv1



## Securing SNMP

### ◆ Setup SNMP Community with an access-list

```
no snmp community public
no snmp community private
access-list 1 permit 1.1.1.1
snmp-server community hard2guess ro 1
snmp-server enable traps snmp authentication
```

### ◆ Setup SNMP Informs

```
snmp-server enable traps
snmp-server host 1.1.1.1 informs version 2c public
```

### ◆ Setup SNMP View

- *SNMP view command can block the user with only access to limited Management Information Base (MIB) information.*

```
snmp-server view MyView ifEntry.*.1 included
snmp-server community hard2guess view MyView ro 1
```

www.ins.com

The knowledge behind the network.®



34

Change default community strings – choose good strings – do not use public/private

**Change community often because it can be seen in clear-text in SNMPv1, former employees**

Watch for SNMP Traps - authenticationFailure – a message was received from an SNMP manager with an invalid community

Source: <<http://www.cisco.com/warp/public/477/SNMP/snmpsecurity-20370.html>>

The Setup SNMP view command can block the user with only access to limited Management Information Base (MIB). It works similar to access-list in that if you have any SNMP View on certain MIB trees, every other tree is denied inexplicably. However, the sequence is not important and it goes through the entire list for a match before it stops.

```
snmp-server community [string] [RO|RW] [AL #]
snmp-server host [ip address] [comm string] < options >
snmp-server trap-authentication
```

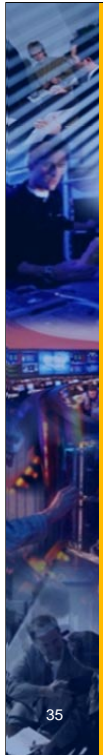
Filter SNMP traffic from only NMS hosts, Ingress Filtering, Egress Filtering

Out-of-Band Management

Protect the NMS systems themselves

Watch out for SNMP running on other ports

- TCP 161 and 162
- TCP and UDP 199 (SNMP Unix multiplexer)
- TCP and UDP 391 (SynOptics SNMP relay port)
- TCP 705 (Agentx)
- TCP and UDP 1993 (Cisco SNMP ports)



## Securing SNMP (cont.)


### ◆ Setup SNMP Version 3

■ *Example :*

```
snmp-server user user1 grp1 v3
snmp-server user user2 grp2 v3
snmp-server user user3 grp3 v3 auth md5 pass3
snmp-server user user4 grp4 v3 auth md5 pass4 priv des56 user4priv
snmp-server group grp1 v3 noauth
snmp-server group grp2 v3 noauth read myview
snmp-server group grp3 v3 auth
snmp-server group grp4 v3 priv
snmp-server view myview mib-2 included
snmp-server view myview cisco excluded
snmp-server community hard2guess RO 10
```

35

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



SNMP version 3 was first introduced in IOS 12.0, but isn't commonly used in network management yet.

The security features provided in SNMPv3 are:

Message integrity—Ensuring that a packet has not been tampered with in-transit.

Authentication—Determining the message is from a valid source.

Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

[http://www.cisco.com/en/US/partner/about/ac123/ac147/ac174/ac202/about\\_cisco\\_ipj\\_archi ve\\_article09186a00800c8396.html](http://www.cisco.com/en/US/partner/about/ac123/ac147/ac174/ac202/about_cisco_ipj_archi ve_article09186a00800c8396.html)

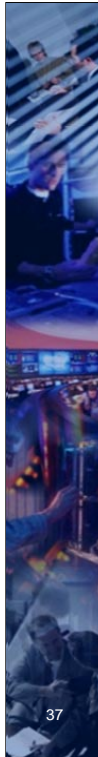
IP Journal Vol1 Issue 3, 1998

## Access

◆ **Before deciding how to control router access, ask these questions?**

- *Who needs access?*
- *When do they need access?*
- *From where do they need access?*
- *During what time schedule do they need access?*





## Basic Authentication

- ◆ **Basic authentication stores passwords as clear text**
- ◆ **Use service password-encryption**
  - *Encrypts passwords using a Vigenere cipher.*
  - *Can be cracked relatively easily*
  - *Does not encrypt SNMP community strings*
- ◆ **Use enable secret <password>**
  - *Encrypts passwords using a MD5 hash*

www.ins.com  
The knowledge behind the network.®



### **enable secret**

The enable secret command is used to set the password that grants privileged administrative access to the IOS system. An enable secret password should always be set. The enable secret should be used, not the older enable password. enable password uses a weak encryption algorithm (see the description of the "service password-encryption" command).

If no enable secret is set, and a password is configured for the console TTY line, the console password may be used to get privileged access, even from a remote VTY session. This is almost certainly not wanted, and is another reason to be certain to configure an enable secret.

### **service password-encryption (and its limitations)**

The service password-encryption command directs the IOS software to encrypt the passwords, CHAP secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder.

However, the algorithm used by service password-encryption is a simple Vigenere cipher; any competent amateur cryptographer could easily reverse it in at most a few hours. The algorithm was not designed to protect configuration files against serious analysis by even slightly sophisticated attackers, and should not be used for this purpose. Any Cisco configuration file that contains encrypted passwords should be treated with the same care used for a clear text list of those same passwords. This weak encryption warning does not apply to passwords set with the enable secret command, but it does apply to passwords set with enable password.

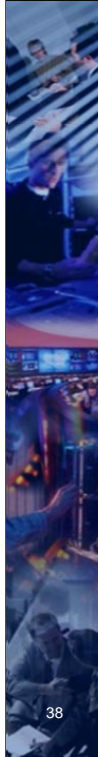
The enable secret command uses MD5 for password hashing. The algorithm has had considerable public review, and is not reversible. It is, however, subject to dictionary attacks (a "dictionary attack" is having a computer try every word in a dictionary or other list of candidate passwords).

It's therefore wise to keep your configuration file out of the hands of untrusted sources, especially if you're not sure your passwords are well chosen. More information about password encryption is available on Cisco's Web site at <http://www.cisco.com/warp/public/701/64.html>.

The following global configuration command encrypts passwords in the written router configurations. Therefore, if the router configuration is copied and listed, the passwords do not appear in the clear-text configuration.

service password-encryption

```
line aux 0
access-class 2 in
transport input all
line vty 0 4
access-class 1 in
-----
```



## Line Authentication (VTY, CON, AUX)

### ◆ Use Access List to control VTY access

```
access-list 1 permit host 10.1.1.2
line vty 0 4
  password 7 12552D23830F94
  exec-timeout 5 0
  access-class 1 in
  login
  transport input telnet ssh
```



### ◆ Control CON access

```
line con 0
  password 7 12552D23830F94
  exec-timeout 5 0
  login
```

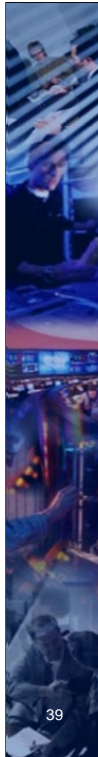
### ◆ Control AUX access

```
line aux 0
  no exec
  exec-timeout 0 0
  no login
  transport input none
  transport output none
```

[www.ins.com](http://www.ins.com)

*The knowledge behind the network.®*





## Secure Shell (SSH)

◆ **SSH is recommended over Telnet**

```
crypto key generate rsa
. . . [2048] . . .

ip ssh time-out 300
ssh authentication-retries 2

aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
username joe password 7 28538539654412

line vty 0 4
transport input none
transport input ssh

show crypto key mypubkey rsa
show ip ssh

% ssh -c des 10.10.10.1
```



39

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®

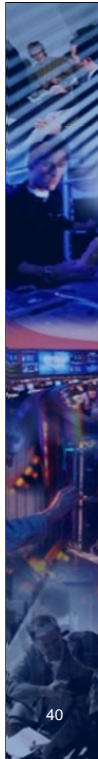


<http://www.atomicgears.com/papers/bastionios.html> – SSH Addendum

DES or 3DES

Cisco SSH Vulnerability

<http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml>



## AAA

- ◆ **Secure user logins with AAA on all ports, virtual and physical**
  - *Local AAA (username)*
  - *RADIUS (Steel Belted Radius)*
  - *TACACS+ (Cisco Secure ACS)*
  
- ◆ **Use privilege levels to control granular access to commands**

40

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



### Console Port

It's important to remember that the console port of an IOS device has special privileges. In particular if a BREAK signal is sent to the console port during the first few seconds after a reboot, the password recovery procedure can easily be used to take control of the system. This means that attackers who can interrupt power or induce a system crash, and who have access to the console port via a hardwired terminal, a modem, a terminal server, or some other network device, can take control of the system, even if they do not have physical access to it or the ability to log in to it normally.

It follows that any modem or network device that gives access to the Cisco console port must itself be secured to a standard comparable to the security used for privileged access to the router. At a bare minimum, any console modem should be of a type that can require the dialup user to supply a password for access, and the modem password should be carefully managed.

Also, set a timeout for the console session so that it will time out and require an authenticated login to regain console access. This following command sets the timeout to 5 minutes:

```
line con 0
exec-timeout 5 0
```

### AUX Port

The use of the AUX port on the border router is not recommended. It is recommended that all access to this port be disabled by using a "no exec" command. The following shows an example of doing this.

```
line aux 0
no exec
```

### VTYs

Defining access-classes to limit access to the vty interfaces on routers is recommended.

The following access list is used to limit vty (i.e. telnet) access to the border router(s) to addresses from [Client]. Telnet connections originating from outside of [Client] will be ignored.

```
access-list 1 permit 12.xx.xx.0 0.0.1.255
access-list 1 deny any any
line vty 0 4
access-class 1 in
```

## AAA Example for TACACS/RADIUS

- ◆ Secure user logins with AAA on all ports, virtual and physical

```
aaa new-model
aaa authentication login default group tacacs+radius local
aaa authorization exec default group tacacs+radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

41

[www.ins.com](http://www.ins.com)

*The knowledge behind the network.®*

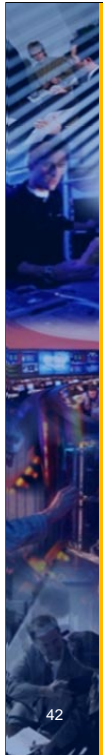


privilege level 1 = non-privileged (prompt is router>), the default level for login

privilege level 15 = privileged (prompt is router#), the level after going into enable mode

privilege level 0 = seldom-used, but includes 5 commands: disable, enable, exit, help, and logout

[http://www.cisco.com/en/US/tech/tk583/tk547/technologies\\_tech\\_note09186a008009465c.shtml](http://www.cisco.com/en/US/tech/tk583/tk547/technologies_tech_note09186a008009465c.shtml)




## HTTP Service

- ◆ There have been known vulnerabilities (buffer overflows) in the HTTP service
- ◆ Don't turn HTTP Services on unless absolutely needed
- ◆ Maybe desirable for some new switch hardware
- ◆ If used secure the access with an ACL

```
no ip http server
ip http access-class ACL#
ip http authentication {aaa/enable/local/tacacs}
ip http port Number
```

42

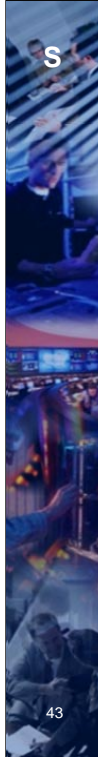
[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



Disable the HTTP server if it not needed by entering the following global configuration command.

```
no ip http server
```

<http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html>



## Routing Protocol Vulnerabilities

- ◆ **Routing protocols deal with re-routing around physical failures and are not robust enough to protect against attackers**
  - *Intended for friendly environments*
- ◆ **Routers advertise themselves by chatting on the network**
  - *Routers show themselves*
  - *Updates, CDP, HSRP, VRRP*
- ◆ **Types of Attacks:**
  - *Routing Disruption Attacks*
    - *Dynamic routing protocols can be exploited*
    - *Traffic could then be re-routed (Transitive Community Modification)*
    - *Routing loop, black-hole, gray-hole, detour, asymmetry, partition*
  - *Resource Consumption/Saturation Attacks*
    - *Injection of extra updates, route requests, or traffic*
    - *Magnified by the presence of loops or detours*
  - *Buffer Overflow Attacks*

www.ins.com  
The knowledge behind the network.®



**Just like HTTP, any protocol the router runs may be vulnerable**

[http://www.sans.org/rr/threats/protocol\\_level.php](http://www.sans.org/rr/threats/protocol_level.php) \*\*\*\*\*

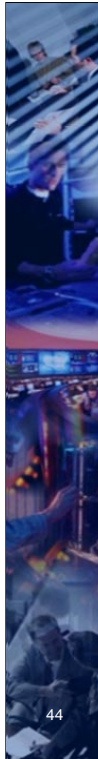
<http://www.sans.org/rr/netdevices/telnet.php>

<http://www.sans.org/rr/netdevices/packet.php>

<http://www.sans.org/rr/protocols/RIP.php>

RIP and OSPF

<http://www.deaddrop.org/security/Papers/ProtectingNetInfrastructure.html>



## BGP-4 Vulnerabilities

- ◆ **BGP-4 peers share updates between them**
  - Assumption is made that peer has authority to send the update and has a correct AS-path
  - Possible to advertise prefix/AS/Path maliciously
- ◆ **BGP-4 peers must be explicitly configured**
  - This limits the threat of a rogue router
  - Masquerading can still be possible
- ◆ **Private peering policies are secret**
  - No authorization for advertisements
- ◆ **BGP Intruders**
  - Subverted BGP speakers, unauthorized BGP speakers, masquerading BGP speakers, subverted links
  - Re-direct traffic for man-in-the-middle attacks or impersonation
- ◆ **One must rely on the filters and routing policy to check what a peer is sending**
- ◆ **BlackHat tools exist and rumors of others spread**
- ◆ **One bad apple can ruin the whole barrel!**



www.ins.com  
The knowledge behind the network.®



“It is really easy to send a TCP RST and drop the BGP session.” **Harder than you think.**

### Successful Spoof may require:

- Match source address
- Match source port
- Match destination port
- Match TTL
- Match Sequence Number

### S-BGP

Origin, Paths, and authorization are verified

Prefix/AS matching with PKI

Add/Withdrawl UPDATE messages are verified

Use a sequence number for messages/UPDATES

Use BGP-4 over IPSec

<http://www.net-tech.bbn.com/sbgp/>


Secure BGP - <http://citeseer.nj.nec.com/kent00secure.html>

<http://www.globecom.net/ietf/draft/draft-murphy-bgp-secr-02.html>

<http://www.net-tech.bbn.com/sbgp/sbgp-index.html>

[http://www.sans.org/rr/protocols/border\\_gate.php](http://www.sans.org/rr/protocols/border_gate.php)

<http://www.academ.com/nanog/feb1998/origin.html>




## Routing Protocol Security

- ◆ Use distribute-lists to control routing updates
- ◆ Use static routes when security is important and connectivity is needed
  - *Internet*
  - *Business partners*
- ◆ Consider placing interfaces in passive
  - passive-interface FastEthernet0/0*
- ◆ Use Out-of-Band (OOB) management to help handle DoS attacks

45

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



### **CenterTrack** - An IP Overlay Network for Tracking Denial-of-Service Floods

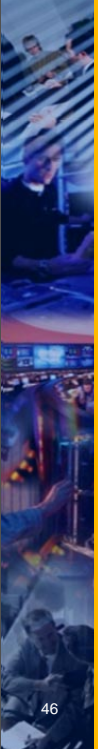
Robert Stone , Internet Security Engineer , UUNET Technologies , NANOG17 , October 5, 1999

[www.silicondefense.com/research/itrex/archive/tracing-papers/stone00centertrack\\_new.pdf](http://www.silicondefense.com/research/itrex/archive/tracing-papers/stone00centertrack_new.pdf)

### **DoSTrack** v2.0 1997 MCI Telecommunications

Code is available at: <ftp://ftp.mci.net/outgoing/dostrack742812.tar>


DoSTracker WEB PAGE is at <http://www.security.mci.net/dostracker>



## Authentication for Dynamic Routing Protocol Updates

- ◆ Don't just route by rumor!
- ◆ Make sure you know to whom you are exchanging routes!
- ◆ Use authentication mechanisms for RIP V2, OSPF, EIGRP and BGP
- ◆ Pre-Shared-Secret keys still have issues
  - Plain-text keys can still be sniffed
  - Use *service password-encryption*
  - Departed employees
- ◆ Use encrypted (MD5) passwords whenever possible
- ◆ Don't hold your breath for PKI/digital certificates
- ◆ Following slides contain examples

[www.ins.com](http://www.ins.com)  
 The knowledge behind the network.®



### From Section 4.4.3 of NSA's Router Security Configuration Guide

#### Router Neighbor Authentication

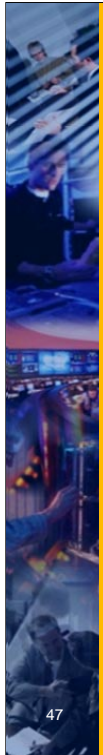
The primary purpose of router neighbor authentication is to protect the integrity of a routing domain. In this case, authentication occurs when two neighboring routers exchange routing information. Authentication ensures that the receiving router incorporates into its tables only the route information that the trusted sending router really intended to send. It prevents a legitimate router from accepting and then employing unauthorized, malicious, or corrupted routing updates that would compromise the security or availability of a network. Such a compromise might lead to re-routing of traffic, a denial of service, or simply giving access to certain packets of data to an unauthorized person.

#### Enhanced User Password Encryption

**username name secret {[0] password | 5 encrypted-secret }**

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a0080087cb1.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cb1.html)

Check the digit preceding the encrypted string in the configuration file. If that digit is a 7, the password has been encrypted using the weak algorithm. If the digit is a 5, the password has been hashed using the stronger MD5 algorithm.



## MD5 for RIPv2

◆ **Configuration Example:**

```


key chain rabbitsfoot
  key 1
    key-string RIPpasswd

interface Loopback0
  ip address 70.70.70.70 255.255.255.255


interface Serial0
  ip address 142.106.0.10 255.255.255.252
  ip rip authentication mode md5
  ip rip authentication key-chain rabbitsfoot

router rip
  version 2
  network 142.106.0.0
  network 70.0.0.0

```



www.ins.com  
The knowledge behind the network.®



MD5 authentication uses the one-way, MD5 hash algorithm, acknowledged to be a strong hashing algorithm. In this mode of authentication, the routing update does not carry the password for the purpose of authentication. Rather, a 128-bit message, generated by running the MD5 algorithm on the password, and the message are sent along for authentication. Thus, it is recommended that you use MD5 authentication over plain text authentication since it is more secure.

**RFC 2082** of RIPv2 with text and keyed MD5 authentication

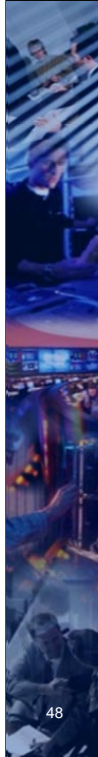
RIP Attacks:

Port scan for UDP 520 - broadcasts

Rprobe.c and srip.c from humble - <http://www.technotronic.com/horizon/ripar.txt>

Nemesis-rip from Mark Grimes

ASS to scan



## MD5 for OSPF

◆ **The following are the commands used for message digest authentication:**

```
ip ospf message-digest-key keyid md5 key
area area-id authentication message-digest
```

◆ **Configuration example:**

```
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip ospf message-digest-key 1 md5 5 mypassword

router ospf 10
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication message-digest
```

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



48

The following are different types of authentication supported by OSPF.

**Null Authentication** - also called Type 0, which means no authentication information is included in the packet header. It is the default.

**Plain Text Authentication** - also called Type 1, it uses simple clear-text passwords.

**MD5 Authentication** - also called Type 2, it uses MD5 cryptographic passwords.

### OSPF Message Digest Authentication

Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet. Unlike the simple authentication, the key is not exchanged over the wire. A non-decreasing sequence number is also included in each OSPF packet to protect against replay attacks.

This method also allows for uninterrupted transitions between keys. This is helpful for administrators who wish to change the OSPF password without disrupting communication. If an interface is configured with a new key, the router will send multiple copies of the same packet, each authenticated by different keys. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new key.

RFC 2154

Port scan for IP protocol 89 to 224.0.0.5

The JiNao team developed and implemented four OSPF attacks. These are basically DOS attacks but may have other applications if other elements of the packets are changed

Max Age attack

Sequence++ Attack

Max Sequence attack

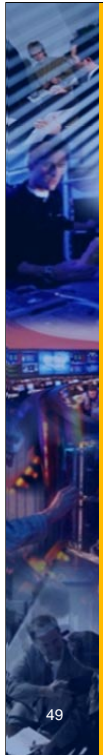
Bogus LSA attack

<http://www.anr.menc.org/projects/JiNao/JiNao.html>

<http://securityresponse.symantec.com/avcenter/security/Content/6895.html>

OSPF vulnerability

Debug ip ospf adj



## MD5 for EIGRP


◆ **Configuration Example:**

```

Interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 holly
key chain holly
key 1
 key-string 123456
  accept-lifetime infinite
router eigrp 1
 network 10.0.0.0
 no auto-summary
 passive-interface default
 no passive-interface FastEthernet0/0

```

www.ins.com  
The knowledge behind the network.®



Q: How to secure IGRP?

A: Change the configs to add an E

IGRP has no security features.

Possible to spoof a metric that is better than the real route

Disruption

Attacker tells R1 that R3 is the best path

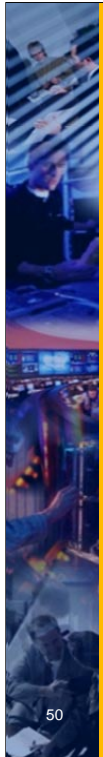
Attacker tells R3 that R1 is the best path

IP EIGRP route authentication provides Message Digest 5 (MD5) authentication of routing updates from the IP EIGRP routing protocol. The MD5 keyed digest in each Enhanced IGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

EIGRP does not use plain text authentication

Port scan for IP protocol 88 to 224.0.0.10

[http://www.cisco.com/en/US/partner/tech/tk648/tk365/technologies\\_security\\_advisory09186a008011c5e1.shtml](http://www.cisco.com/en/US/partner/tech/tk648/tk365/technologies_security_advisory09186a008011c5e1.shtml)




## MD5 for BGP

- ◆ **Configuration example:**
- ◆ **The following example specifies that the router and its BGP peer at 145.2.2.2 invoke MD5 authentication on the TCP connection between them:**

```
router bgp 109
 neighbor 145.2.2.2 password mypasswd
```
- ◆ **Enable route dampening to minimize instability due to route flapping (RFC 2439)**

```
router bgp 109
 bgp dampening
 show ip bgp flap-statistics
```
- ◆ **BGP Filtering**
  - Filter for Bogons
  - Use Communities

[www.ins.com](http://www.ins.com)  
 The knowledge behind the network.®



BGP only uses MD5 Authentication - RFC2385

Cisco Packet Magazine: Why Authenticate BGP Routers

<http://www.cisco.com/warp/public/784/packet/jul02/techspeak.html>

Rob's Secure BGP Template

<http://www.cymru.com/Documents/secure-bgp-template.html>

MD5 on BGP4 connections (help with RST attacks)

RFC2726 - PGP Authentication for RIPE Database Updates

Port scan for TCP port 179

```
[root@premis]# nmap -sS -p 179 -v router.ip.address.2
```

Interesting ports on (router.ip.address..2):

```
Port      State  Service
179/tcp   open   bgp
```

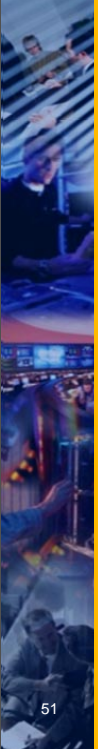
-An open BGP port. More vulnerable to attack.

```
[root@premis netw3]# nmap -sS -n -p 179 router.ip.address.6
```

Interesting ports on (router.ip.address.6):

```
Port      State  Service
179/tcp   filtered  bgp
```

A BGP port that is filtered. More resistant to attack.




## HSRP Vulnerabilities

- ◆ HSRP vulnerabilities are publicized
- ◆ Authentication string is in clear-text
- ◆ Code has been written to spoof HSRP packets
- ◆ Attackers sends “coop” and pre-empts other HSRP routers to assume the “active” role
- ◆ Used for DoS or Man-in-the-middle attack
- ◆ Mitigation through configuration and use of IPSec
  - Set the standby priority to 255 on your routers
  - Use IP addresses X.X.X.254, .253 for the legitimate router IPs so they take precedence over the attacker

51

www.ins.com  
The knowledge behind the network.®



Dugan p 58

HSRP uses UDP on port 1985 to multicast address 224.0.0.2

Authentication in clear text

Hello packets

Attacker advertises higher priority and preempts the active router

Consider VRRP – it uses authentication

**vrrp [address | advertisement-interval | authentication | exit | preempt | priority | shutdown | track]**

```
interface Ethernet0
```

```
ip address 171.16.6.5 255.255.255.0
```

```
no ip redirects
```

```
standby 1 ip 171.16.6.100
```

```
standby 1 priority 105
```

```
standby 1 preempt
```

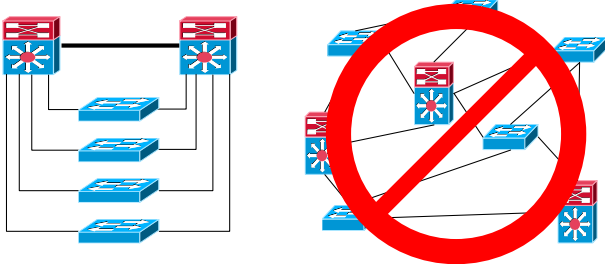
```
standby authentication string
```

Debug standby

W


## Layer 2 – Start Things Out Right

- ◆ Plan with security in mind
- ◆ Good Designs simplify security
- ◆ KIS Principle – Keep It Simple



- ◆ **Isolate Default VLANs from Trunks**
  - VLAN1 – The Dead VLAN
  - VLAN 1001–1005 : The Dead Technology VLANS

www.ins.com  
The knowledge behind the network.®

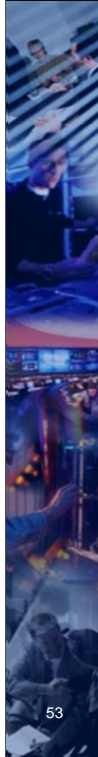


52

Stephen Dugan, CCSI

Presentation to BlackHat Briefings

<http://www.blackhat.com/html/bh-asia-02/bh-asia-02-speakers.html#Steve%20Dugan>



## Layer 2 – Vulnerabilities?

### ◆ VLAN Hopping

- *Modify tags on a trunked port*

### ◆ How to Make a Switch Act Like a Hub

- *Flood as switch with random MAC Addresses*
- *Forces switch to flood all packets to all ports*

### ◆ Network Sniffing with Switch Port

- *Requires arp spoofing tool with bridging software*
- *Send continuous arp replies to client on part of server convincing client that the interceptor is the server*
- *Bridges traffic between client and server to insure apparently normal communication flow*

53

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®



Phrack Volume 0x0b, Issue 0x39, Phile #0x06 of 0x12 - Taranis

Phrack Volume 0x0b, Issue 0x3c, Phile #0x07 of 0x10 – Burning the bridge

Phrack Volume 0xa, Issue 0x38, 05.01.2000 0x0a[0x10] – Things to do in Cisco Land



## Layer 2 – Basic Prevention

- ◆ **Management VLAN**
  - Change default to a randomly selected that is the same across all switches
  - Do not place users on VLAN
- ◆ **Explicitly configure ports**
  - `set port host <mod/port>`
    - Turn trunking off / Turn portfast on
- ◆ **Enable Port Level Security**
- ◆ **Disable unused ports**
  - `set port disable <mod/port>`
- ◆ **Turn on BPDU Guard**
  - `set spantree portfast bpdu-guard enable`

www.ins.com  
The knowledge behind the network.®



[http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_tech\\_note09186a008009482f.s.html](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.s.html)

### portfast Bridge Protocol Data Unit (BPDU) guard

#### Prerequisites

STP portfast BPDU guard was first introduced in the following versions:

Version 5.4.1 of the Catalyst software for Catalyst 4000 (Supervisor II), 5000, and 6000 platforms

Version 12.0(7)XE of the Cisco IOS® software (Native IOS) for the Catalyst 6000 platforms

Version 12.1(8a)EW of the Cisco IOS Software for the Catalyst 4000 Supervisor III

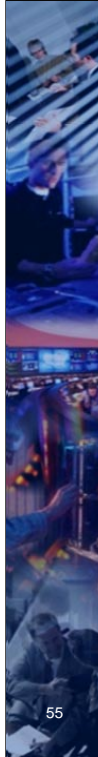
Version 12.1(12c)EW of the Cisco IOS software for the Catalyst 4000 Supervisor IV

Version 12.0(5)WC5 of the Cisco IOS software for the Catalyst 2900XL and 3500XL series

Version 12.1(4)EA1 of the Cisco IOS Software for the Catalyst 3550 series switches

Version 12.1(6)EA2 of the Cisco IOS software for the Catalyst 2950 series switches

STP portfast BPDU guard is *not* available for the Catalyst 8500 series, the 2948G-L3 or 4908G-L3, or any other Catalyst switch not mentioned above.



## Layer 2 – More Advance Prevention

### ◆ VTP – VLAN Trunking Protocol

- *AKA - The Cisco Layer 2 Hackers Favorite DOS Tool!*
- *Intended to maintain VLAN consistency*
- *Risky to use under normal conditions*
- *Set all switches to VTP Transparent Mode*

### ◆ DTP – Dynamic Trunking Protocol

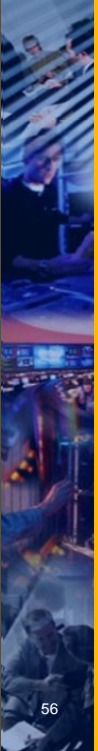
- *The Question - To Trunk or Not to Trunk*
- *Can be manipulated to access all VLANS without the need for a router*
- *Set DTP ON/ON for all trunk ports*
- *Set DTP OFF/OFF for all non-trunk ports*

55

[www.ins.com](http://www.ins.com)



*The knowledge behind the network.®*






## Non-Cisco security tools

- ◆ **Nmap** – Port scanning & fingerprinting
- ◆ **Ndiff** – Compares nmap output for diffs
- ◆ **Netcat** – Opening sockets & port scanning
- ◆ **Nessus** – Vulnerability scanner
- ◆ **Ncat** – Evaluates configs against the “Secure IOS Template”

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*



Reference to Scott’s Troubleshooting presentation for NetCat slide 51

<http://www.nmap.org>

# **nmap -sT 10.10.1.1 -p 1-65535**                   **TCP Scan**

# **nmap -sU -p 1-65535 10.10.1.1**                   **UDP Scan**

<http://www.vinecorp.com/ndiff>

<http://www.hackers.com/new/>

<http://www.nessus.org/>

<http://www.laurentconstantin.com/en/lcrzoex/>

<http://online.securityfocus.net/>

<http://ncat.sourceforge.net/>

[http://www.iss.net/products\\_services/enterprise\\_protections/vulnerability\\_assessment/](http://www.iss.net/products_services/enterprise_protections/vulnerability_assessment/)

<http://www.wwdsi.com/saint/index.html>

<http://www.porcupine.org/satan>

<http://www.nessus.org/>

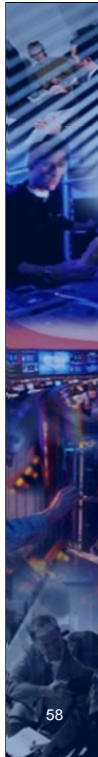


## References

- ◆ **Secure IOS Template, Rob Thomas**
  - <http://www.cymru.com/Documents/secure-ios-template.html>
- ◆ **Router Security Configuration Guide, NSA**
  - <http://svcaacs.conxion.com/cisco/>
- ◆ **Increasing Security on IP Networks, Cisco**
  - <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2016.pdf>
- ◆ **Improving Security on Cisco Routers**
  - <http://www.cisco.com/warp/public/707/21.html>

[www.ins.com](http://www.ins.com)  
The knowledge behind the network.®





## Questions?

### ◆ Contact Information:

- **William H. Gilmore**  
*william.gilmore@ins.com*
- **Scott R. Hogg**  
*scott.hogg@ins.com*



58

[www.ins.com](http://www.ins.com)  
*The knowledge behind the network.®*

