

Securing Network Devices

October 21, 2014

Lecture topics, in detail

- ▶ Design strategies in secure networks;
- ▶ Securing router administration access;
- ▶ User login security enhancements;
- ▶ Using SSH for remote management;
- ▶ Securing Cisco IOS image and configuration files;
- ▶ SNMP;
- ▶ Syslog;
- ▶ NTP;
- ▶ Locking down a router with AutoSecure;

Previous IOS experience

- ▶ This course is focused on configuring Cisco devices
 - ▶ Mapped on the CCNA Security
- ▶ A basic understanding of IOS command syntax is required

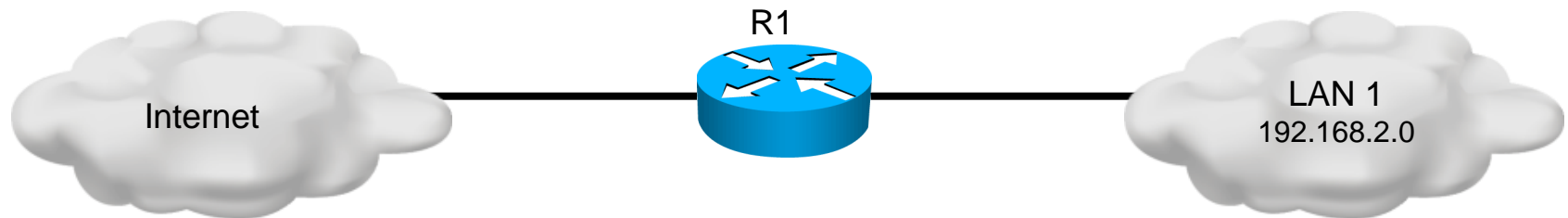
Securing the network

- ▶ Securing a network basically means:
 - ▶ Securing the edge router
- ▶ What is an edge router?
 - ▶ Yeah, a router at the edge... but an edge between what?
- ▶ An edge router is the last router between the local network and the “danger” zone – the Internet
- ▶ First and last line of defense
- ▶ There is no universal security design;
 - ▶ Security is dictated by the company’s policy
...and by your skills...

Securing the edge router

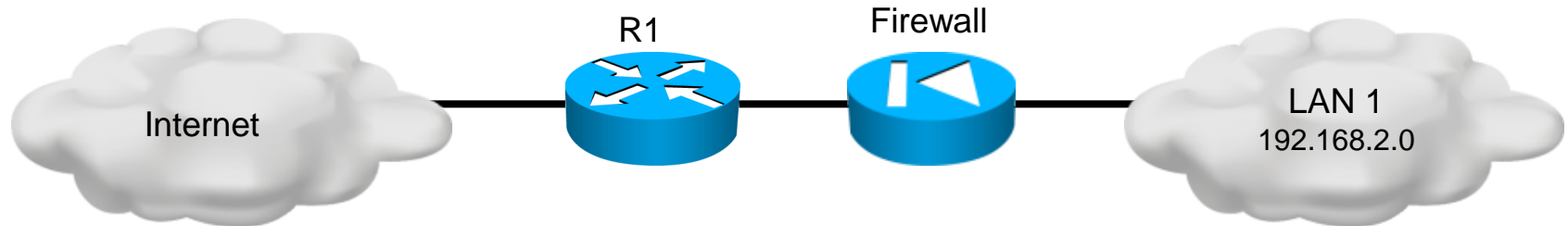
- ▶ The edge router is the most exposed one
 - ▶ You need to secure pretty much everything!
 - ▶ Ensure physical security
 - ▶ Operating system security
 - ▶ Administrative access security
 - ▶ Remote access security
- ▶ First, design the perimeter architecture:
 - ▶ There are different implementations

Perimeter – Single router approach



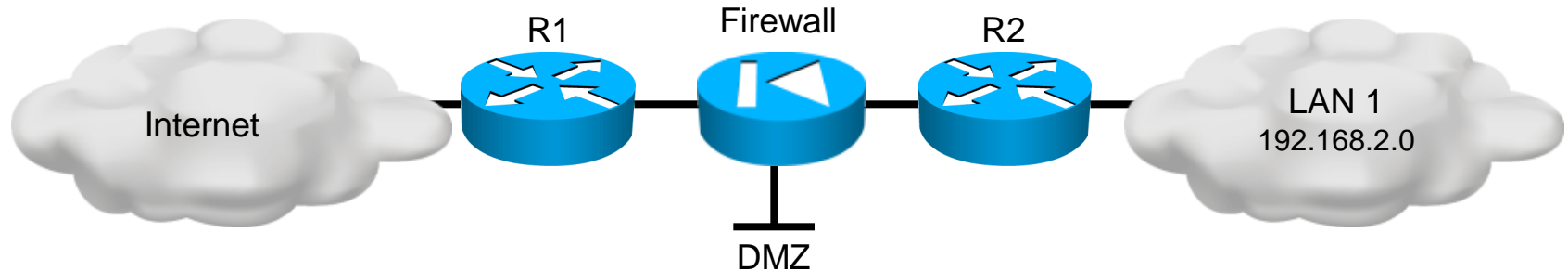
- ▶ A single router between the LAN and the Internet
- ▶ The router has all the security policies and traffic filtering mechanism configured
- ▶ This approach might not always be the best...

Perimeter – Defense-in-depth approach



- ▶ Rules in the router determine what traffic can pass
- ▶ All passing traffic is filtered through the firewall
- ▶ Can have multiple layers of routers and firewalls
 - ▶ Each layer can defend the network using different methods

Perimeter – DMZ approach



- ▶ A neutral zone between the private and the public network
- ▶ Used for public servers, accessible from the Internet
- ▶ Cannot initiate sessions to the private network
 - ▶ In case the DMZ is compromised, the LAN should still be secure

Ensuring the security of a router

▶ Securing access

- ▶ Thoroughly secure administrative access and authentication
- ▶ Disable anything unused: ports, services, accounts
- ▶ Log and account all accesses

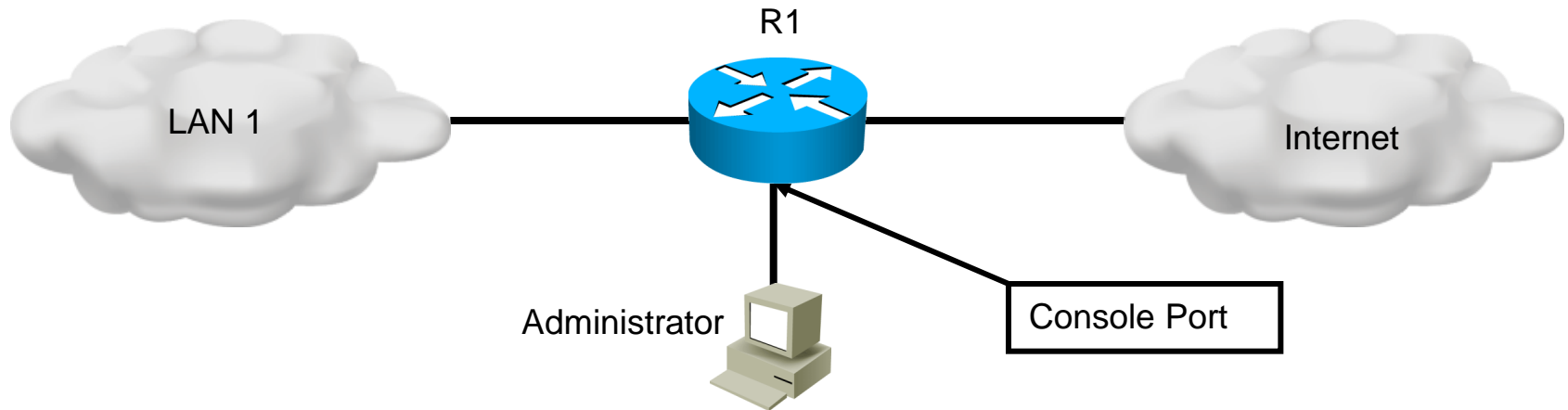
▶ Securing the operating system

- ▶ Always use the latest stable version
- ▶ Backup the operating system and its configuration

▶ Physical security

- ▶ Routers should be placed in secure locations
- ▶ Install an uninterruptible power source

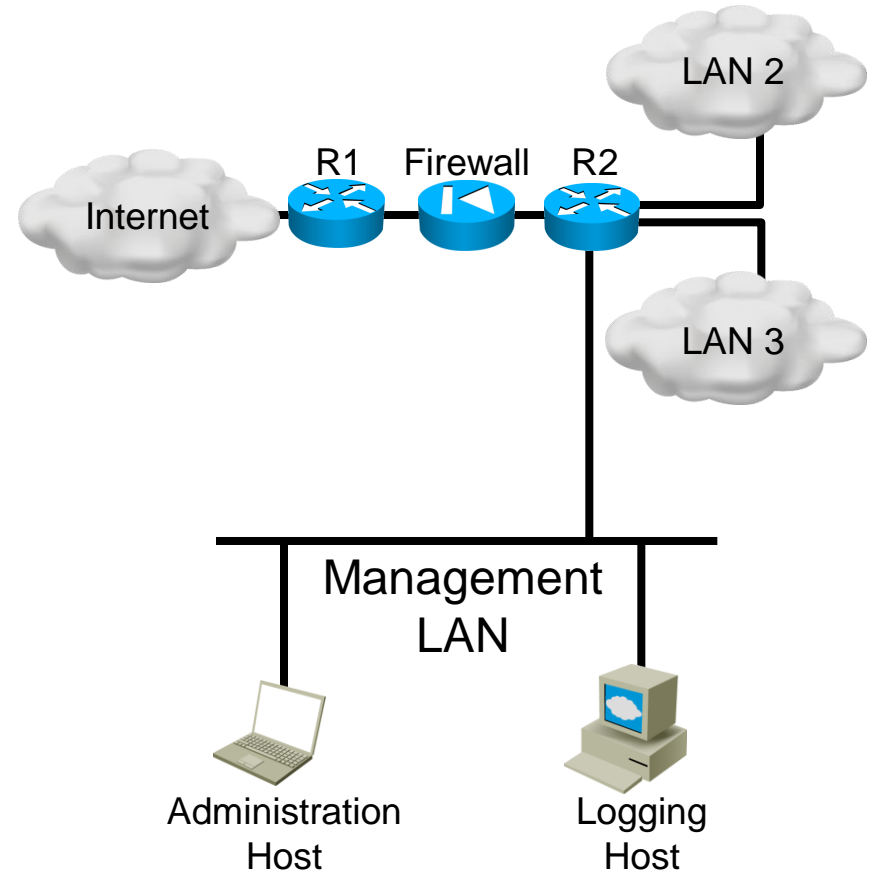
Types of access – local access



- ▶ Requires a direct connection to the device
- ▶ Cisco routers use console and AUX ports
- ▶ The administrator requires only a terminal software
 - ▶ Xterm, Putty, etc.

Types of access – remote access

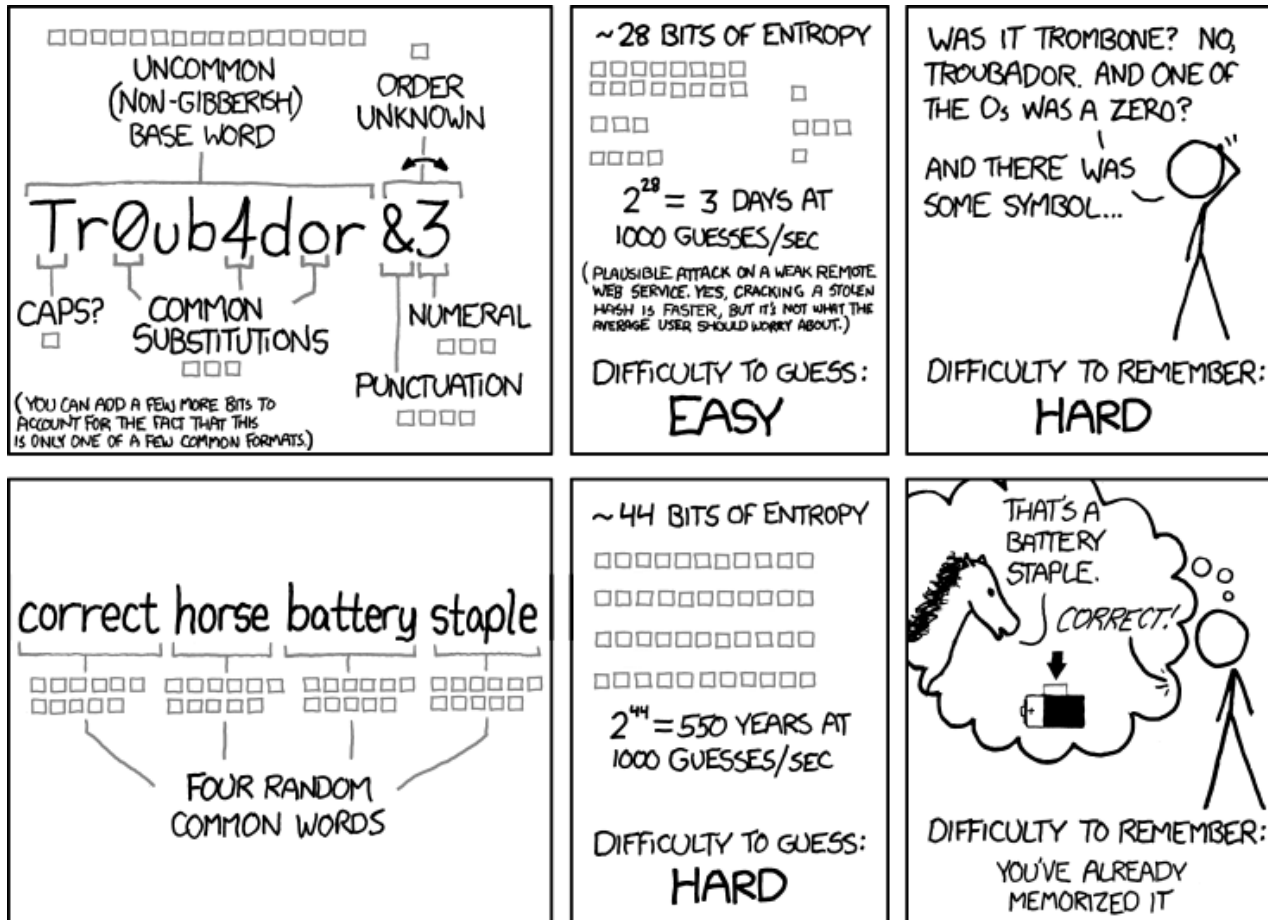
- ▶ **Protocols used:**
 - ▶ Telnet, SSH for direct CLI access
 - ▶ SNMP for centralized device management



Protecting access with passwords

- ▶ All access methods can be password-protected
- ▶ Strong passwords eliminate the risk of dictionary attacks
 - ▶ Lowercase, uppercase, numbers, special characters
 - ▶ Length > 10
 - ▶ Avoid commonly used words
 - ▶ Avoid repetitions
- ▶ Passwords must be changed often
 - ▶ This should be stated in the security policy
- ▶ Of course, try not to write them down all around you

Protecting access with passwords



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Configuring access passwords

- ▶ Restricting access to privileged mode:

```
R1(config)# enable password cisco2
```

or

```
R1(config)# enable secret cisco1
```

(note that you cannot set the same password in both ways)

- ▶ The difference?

- ▶ In the configuration file you'll see:

```
R1#show run | include enable  
enable secret 5 $1$W5ah$mNNIchs14INIQcQR2qWU1/  
enable password cisco2
```

Configuring access passwords

- ▶ Protecting incoming Telnet & SSH connections:

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
```

- ▶ By default, Cisco routers support up to 5 simultaneous Telnet or SSH sessions
- ▶ Protecting console and AUX access:

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line aux 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#
```

Configuring secure administration

- ▶ Securing password-protected administration by implementing the following procedures:
 - ▶ Ensure a minimum password length is used:

```
R1(config)#security password min-length 8
R1(config)#enable secret cisco
% Password too short - must be at least 8 characters.
Password configuration failed
```
 - ▶ Passwords already in place are unaffected
 - ▶ The minimum password length can be set between 0 and 16 characters

Configuring secure administration

- ▶ Disable idle connections – inactivity timer
 - ▶ Idle connections automatically disconnect after 10 minutes (default)
 - ▶ An attacker has a window of opportunity to gain privileges

```
R1(config)#line console 0
R1(config-line)#exec-timeout 3 30
```
 - ▶ For a secure lab environment you can use the values “0 0”
- ▶ Disable unused connection lines
 - ▶ The no exec command will not start an exec (command line process) on a specific line

```
R1(config)#line vty 0 5
R1(config-line)#no exec
R2#telnet 10.0.0.1
Trying 10.0.0.1 ... Open
[Connection to 10.0.0.1 closed by foreign host]
```

Configuring secure administration

- ▶ Encrypt clear-text passwords:

```
R1(config)#service password-encryption
```

- ▶ The configuration file is a little bit “safer” now:

- ▶ Type-7 encryption is an extremely weak method

```
R1#show running-config
```

```
line con 0
```

```
password 7 110A1016141D4B
```

```
line vty 0 4
```

```
password 7 02050D480809
```

- ▶ The algorithm is quickly reversible
- ▶ Useful only for preventing unauthorized individuals from viewing the configuration file
- ▶ “no service password-encryption” command disables the encryption, but passwords already encrypted will remain the same

User creation

- ▶ User can have different privileges

- ▶ Syntax:

```
R1(config)#username Robert secret ?
```

```
0      Specifies an UNENCRYPTED secret will follow
```

```
5      Specifies a HIDDEN secret will follow
```

```
LINE   The UNENCRYPTED (cleartext) user secret
```

```
R1(config)#username Robert password ?
```

```
0      Specifies an UNENCRYPTED password will follow
```

```
7      Specifies a HIDDEN password will follow
```

```
LINE   The UNENCRYPTED (cleartext) user password
```

- ▶ To use the local user database instead of the line/console password (in line configuration mode):

```
R1(config-line)#login local
```

Login security enhancements

- ▶ All enhancements have to be enabled
- ▶ The block-for command:

```
R1(config)#login block-for 100 attempts 7 within 60
```

 - ▶ Blocks all login attempts for 100 seconds if 7 login attempts were failed within 60 seconds
 - ▶ The 100-second delay is also known as the “quiet period”
- ▶ The “block-for” command only applies to Telnet and SSH (not console logins)
- ▶ A failed attempt means a bad username/password combination

Login security enhancements (2)

- ▶ To generate log messages for successful/failed logins use:

```
R1(config)#login on-failure log
```

```
R1(config)#login on-success log
```

- ▶ To generate a message when a failure rate is exceeded

```
R1(config)#security authentication failure rate 10 log
```

- ▶ Sends a log message whenever 10 failed login attempts are detected within one minute.

- ▶ To force a login delay (seconds), regardless of valid/invalid login credentials:

```
R2(config)#login delay 2
```

- ▶ Slows down brute force attacks
 - ▶ BF attacks test 1000 of passwords/sec

Checking login failures

- ▶ “show login” summarizes the login configuration:

R2#show login

A login delay of 2 seconds is applied.

No Quiet-Mode access list has been configured.

Router enabled to watch for login Attacks.

If more than 7 login failures occur in 60 seconds or less,
logins will be disabled for 100 seconds.

Router presently in Normal-Mode.

Current Watch Window

Time remaining: 4 seconds.

Login failures for current window: 6.

Total login failures: 6.

These are your failures



Checking login failures

- ▶ “show login failures” shows... exactly what it says...

```
R2#show login failures
```

```
Total failed logins: 6
```

```
Detailed information about last 50 failures
```

Username	SourceIPAddr	lPort	Count	TimeStamp
rrazvan	10.0.0.1	23	1	00:38:16 UTC Fri Oct 16 2009
doggy	10.0.0.1	23	1	00:38:19 UTC Fri Oct 16 2009
buzz	10.0.0.1	23	1	00:38:27 UTC Fri Oct 16 2009
hacker	10.0.0.1	23	1	00:38:34 UTC Fri Oct 16 2009
evil	10.0.0.1	23	1	00:38:37 UTC Fri Oct 16 2009
nasty	10.0.0.1	23	1	00:38:40 UTC Fri Oct 16 2009

Commonly used hacker names...

Configuring banners

- ▶ A banner's role is to inform potential intruders that they are not welcomed on the network
 - ▶ Their importance is legal-based
 - ▶ Court cases have been won because intruders encountered a "Welcome!" banner

- ▶ Example configuration of a message-of-the-day banner:

```
R2(config)#banner motd & Access to this private equipment is restricted.
```

```
Enter TEXT message. End with the character '&'.
```

```
All unauthorized access will be prosecuted to the fully extent of law.&
```

- ▶ Banners can span multiple lines
- ▶ Start and end with the same character

Configuring banners

- ▶ Also, certain “variables” can be used inside a banner:
 - ▶ `$(hostname)` – displays the router’s hostname
 - ▶ `$(domain)` – displays the router’s domain name
 - ▶ `$(line)` – displays the current vty line
 - ▶ `$(line-desc)` – displays the line description (if set)

Securing remote access

- ▶ The Telnet protocol transmits unencrypted data over TCP port 23
- ▶ Traffic (router configurations, commands, etc) can be easily sniffed
- ▶ Solutions:
 - ▶ Disable Telnet and use only the good 'old console..
 - ▶ Realize that remote access IS A MUST and use something else
- ▶ SSH (Secure SHell) provides remote authentication and encryption
 - ▶ Not all IOS images support SSH connections
 - ▶ Look for “k8” or “k9” in the image’s filename
 - ▶ Example: c3640-jk9o3s-mz.123-22.bin

Prepare for SSH!

- ▶ Things to check before configuring a router for SSH access:
 - ▶ Make sure the IOS image supports SSH
 - ▶ Make sure the router has a unique hostname
 - ▶ Make sure the router has the correct domain name of the network
 - ▶ Make sure that you have at least a valid user configured on the router (or that the router uses AAA for authentication)
 - ▶ More on AAA in a later course

Steps for configuring SSH

► Check the IOS image:

```
R2#show version | include IOS
```

```
IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.3(22),  
  RELEASE SOFTWARE (fc2)
```

► Configure a domain name:

```
R2(config)#ip domain-name my.home
```

► Generate RSA private/public key pair:

```
R2(config)#crypto key generate rsa general-keys modulus 1024
```

```
The name for the keys will be: R2.my.home
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys ...[OK]
```

```
R2(config)#
```

```
*Oct 19 00:17:23.487: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

Steps for configuring SSH

- ▶ Create at least a valid username:

```
R2(config)#username student secret poli
```

- ▶ Activate the SSH protocol for the virtual lines (vty):

```
R2(config)#line vty 0 4
```

```
R2(config-line)#transport input ssh
```

- ▶ Test your connection:

```
R1#ssh ?
```

```
-c      Select encryption algorithm
```

```
-l      Log in using this user name
```

```
-o      Specify options
```

```
-p      Connect to this port
```

```
WORD   IP address or hostname of a remote system
```

```
R1#ssh -l student 10.0.0.2
```

```
Password:
```

```
R2>
```

Other SSH commands

- ▶ Setting the SSH version

- ▶ 2 is more secure than 1 – uses Diffie-Helman key exchange and MAC (Message Authentication Code)

```
R2(config)#ip ssh version 2
```

- ▶ Specify an interval for the SSH sessions timeout:

```
R2(config)#ip ssh time-out 60
```

- ▶ The default is 120 seconds

- ▶ Set the number of authentication retries:

```
R2(config)#ip ssh authentication-retries 5
```

- ▶ The default is 3 retries

SSH “show” commands

- ▶ Viewing the active connections:

```
R2#show ssh
```

Connection	Version	Encryption	State	Username
0	1.5	3DES	Session started	student

- ▶ Displaying the current SSH configuration

```
R2#show ip ssh
```

```
SSH Enabled - version 1.5
```

```
Authentication timeout: 30 secs; Authentication retries: 5
```

- ▶ Viewing your generated RSA public key:

```
R2#show crypto key mypubkey rsa
```

Privilege levels

- ▶ Privilege levels exist because complete access should not be given to everyone
- ▶ You have met so far two privilege levels:
 - ▶ User EXEC mode (privilege level 1)
 - ▶ The default level for login; you cannot change any configuration or view the current configuration file
 - ▶ Privileged EXEC mode (privilege level 15)
 - ▶ Reserved for the “enable” command. Users can change any configuration and view any configuration file
- ▶ But there are others:
 - ▶ Level 0:
 - ▶ predefined, includes only enable, disable, exit, help, logout
 - ▶ Levels 2-14: can be customized

Privilege commands examples

- ▶ Creating a user with a privilege level of 5:

```
R2(config)#username support privilege 5 secret cisco
```

- ▶ Setting the level 5 secret password:

```
R2(config)#enable secret level 5 LetMeIn
```

- ▶ Allowing the show startup-config command for the privilege level 5:

```
R2(config)#privilege exec level 5 show startup-config
```

Privilege commands examples

- ▶ Commands like:

- ▶ `R2(config)#username support privilege 5 secret cisco`

- automatically put the user in the specified privilege level at login

- ▶ Commands are allowed per privilege mode, not per user

- ▶ Any user can change its privilege mode using:

- `enable 5`

- ▶ The “enable” you knew until now was a synonym for:

- `enable 15`

- ▶ Privilege modes can be password-protected (see previous slide)

- ▶ To view your current privilege level:

- `R2#show privilege`

- `Current privilege level is 5`

Privilege level limitations

- ▶ You cannot restrict access to interfaces, lines, ports or logical interfaces on the router
- ▶ Commands available on one privilege level will be automatically available on superior privileges, too

which also means that...

- ▶ Commands available on one privilege level will NOT be available for lower privilege levels

Protecting the IOS and its configuration

- ▶ If attackers gain access to a router, there are many things they can do (or destroy)
- ▶ (A quick) one of them is to completely erase the IOS and the configuration
 - ▶ Reinstalling the IOS image and recovering the configuration file from a backup creates high network downtime
- ▶ The Cisco IOS Resilient Configuration allows faster recovery:
 - ▶ The system secures the IOS image and the configuration
 - ▶ Any attempts to delete, replace or modify the IOS are denied
 - ▶ A secure copy of the startup config is also backed up

Securing the IOS and its configuration

- ▶ The saved IOS and configuration file are called “bootset”

- ▶ To secure the IOS image:

```
Router(config)#secure boot-image
```

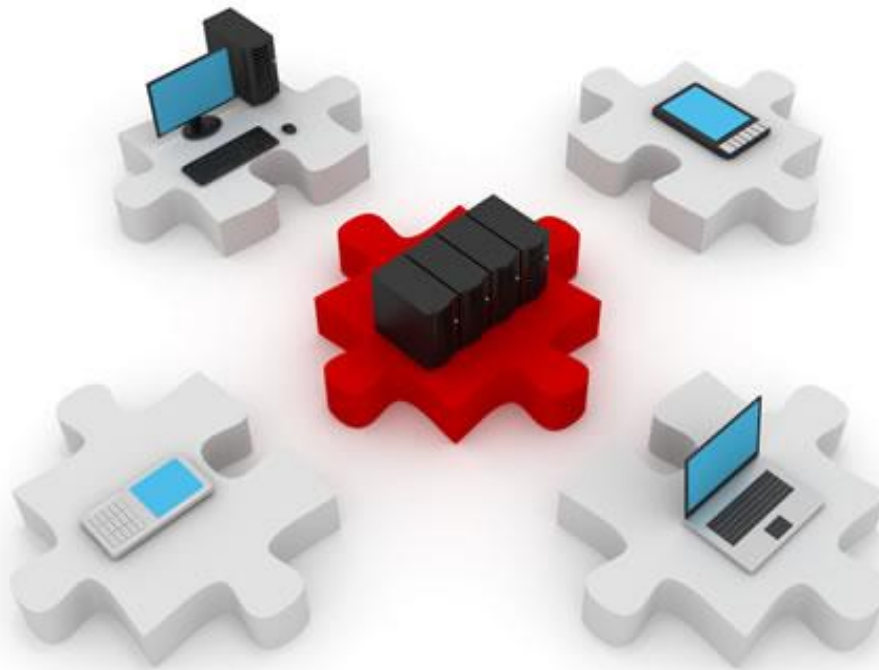
- ▶ Only locally stored images can be secured
- ▶ The backup copy can be stored only locally

- ▶ To secure the startup configuration:

```
Router(config)#secure boot-config
```

- ▶ Neither the backed-up IOS or the configuration file are visible in the file system
- ▶ Unsecuring the bootset requires console access
- ▶ To view the IOS/configuration resilience options:

```
Router#show secure bootset
```



Secure management and logging

See what's happening on the network

Methods for management and logging

- ▶ Consider the network management traffic
 - ▶ Out-of-band (OOB)
 - ▶ Information flows on a dedicated management network, without any production traffic
 - ▶ In-band
 - ▶ Information flows across the production network, using the same channels
- ▶ A device might not have enough interfaces for OOB
- ▶ If management traffic must go across the production network, it is recommended to use an encrypted tunnel
 - ▶ The tunnel must only allow management traffic

Threatening the management network

- ▶ If a dedicated management network exists, then it is an attractive target for hackers
 - ▶ It spans all over the network
 - ▶ It contains information about all the devices in the network
 - ▶ If unsecured, a hacker can use it to take control of the network

SNMP

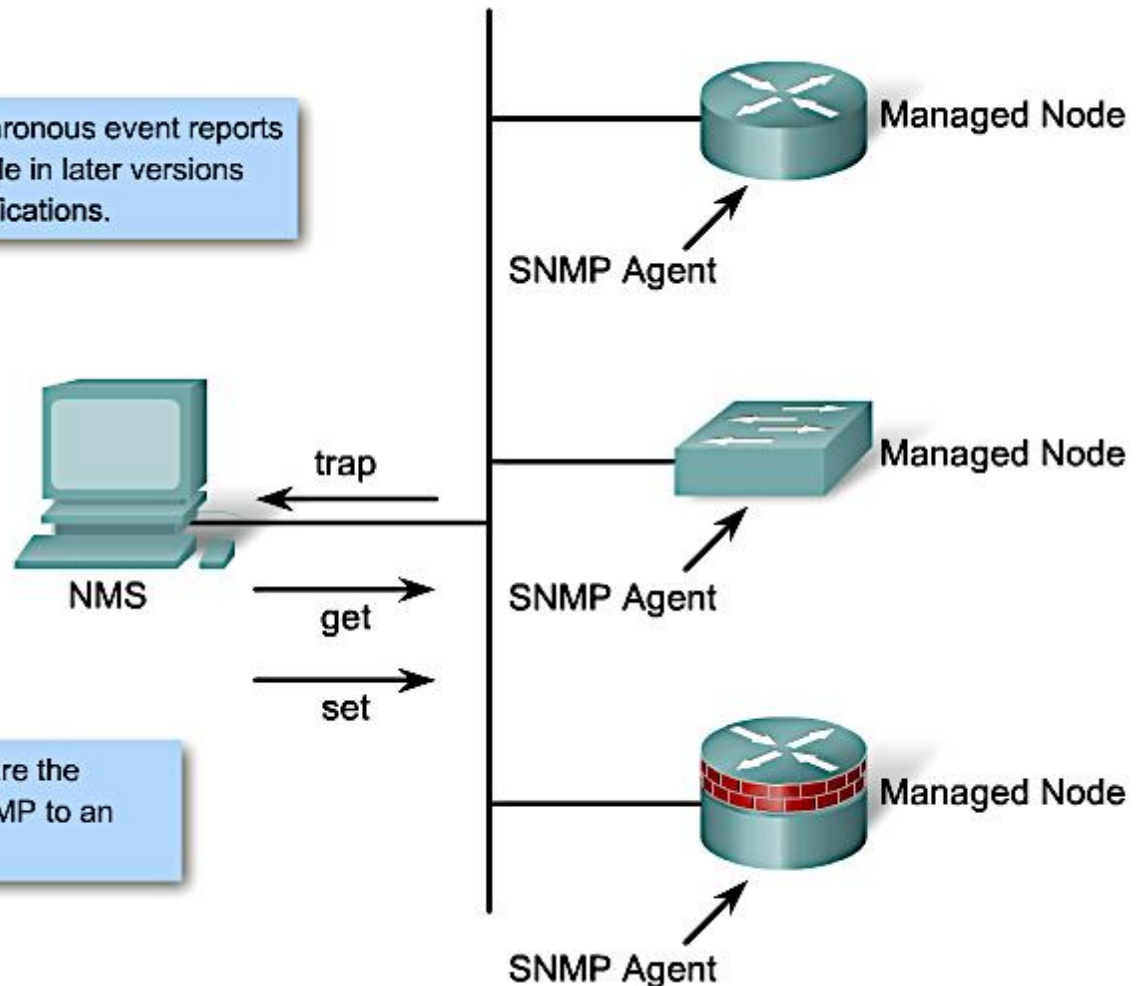
- ▶ Simple Network Management Protocol
- ▶ Runs at the application layer
- ▶ Manages network “nodes”
 - ▶ Nodes are routers, switches, hubs, servers, workstations, security appliances.
- ▶ Enables remote administration for these devices
- ▶ Community strings
 - ▶ Used for authentication
- ▶ Multiple versions available: v1, v2, v3
 - ▶ Only version 3 offers strong authentication and encryption

SNMP basic concepts

- ▶ **Managing systems (Masters)**
 - ▶ Administrative computers that monitor a group of devices
 - ▶ Also called NMS (Network Management System)
- ▶ **Managed systems (Slaves)**
 - ▶ A device that runs an Agent
- ▶ **Agent**
 - ▶ Software component running on slave systems that reports data back to the master system
 - ▶ The agent uses SNMP to communicate
 - ▶ Exposes data as variables: “name”, “free memory”, “processes”
 - ▶ Can receive and apply new configurations

SNMP messages

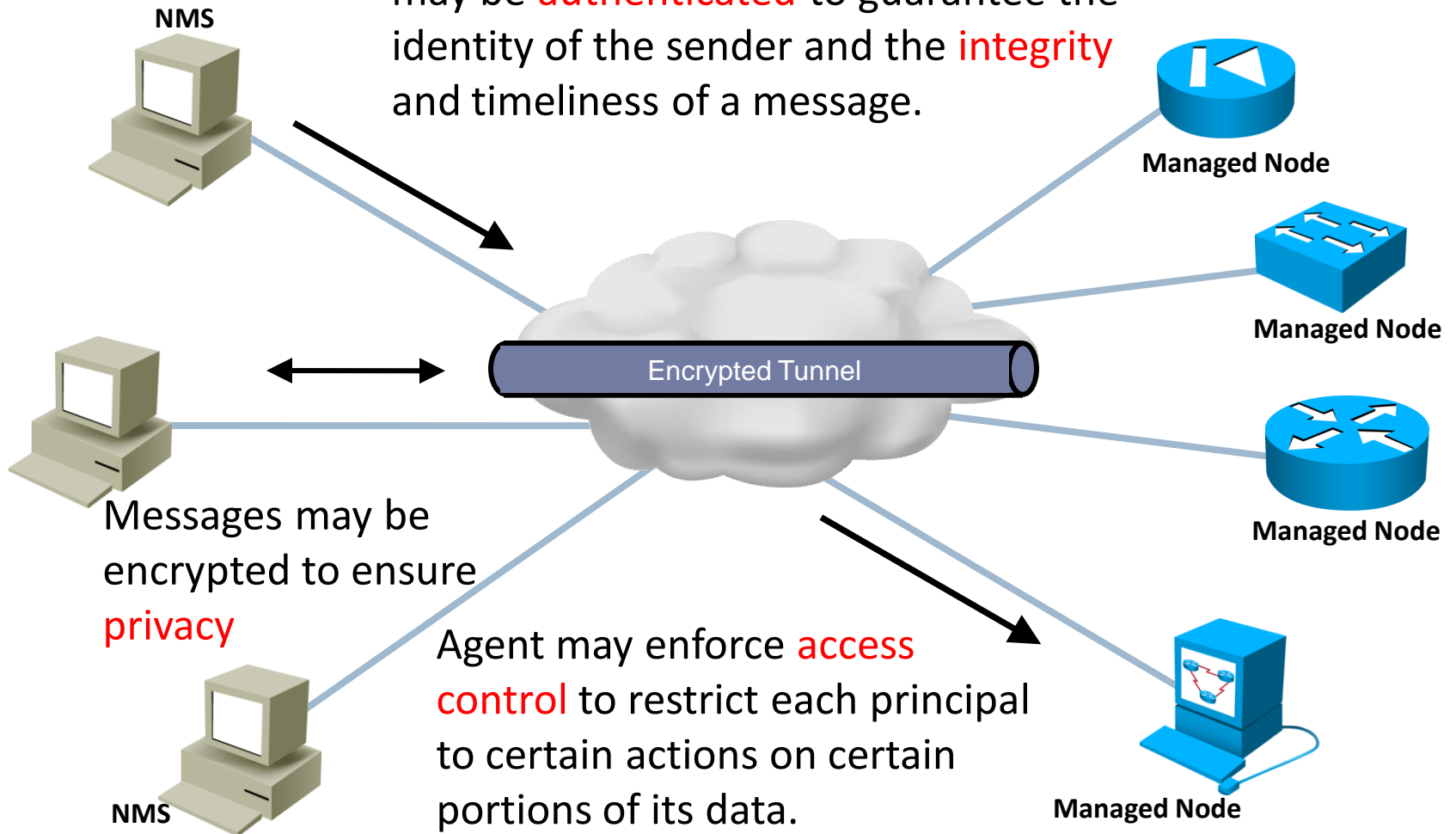
In SNMPv1, asynchronous event reports are called **traps** while in later versions they are called **notifications**.



The actions **GET** and **SET** are the vulnerabilities that open SNMP to an attack.

SNMPv3

Transmissions from manager to agent may be **authenticated** to guarantee the identity of the sender and the **integrity** and timeliness of a message.



SNMP levels of security

- ▶ SNMP v1 and v2 only support:
 - ▶ noAuthNoPriv: only use community string, no authentication or encryption
- ▶ SNMP v3 allows for the following levels of security:
 - ▶ noAuthNoPriv: authenticates a packet only by community string or username
 - ▶ authNoPriv: authenticates a packet using HMAC-MD5 or HMAC-SHA
 - ▶ authPriv: Authenticates a packet just like Auth but also provides encryption using DES, 3DES or AES

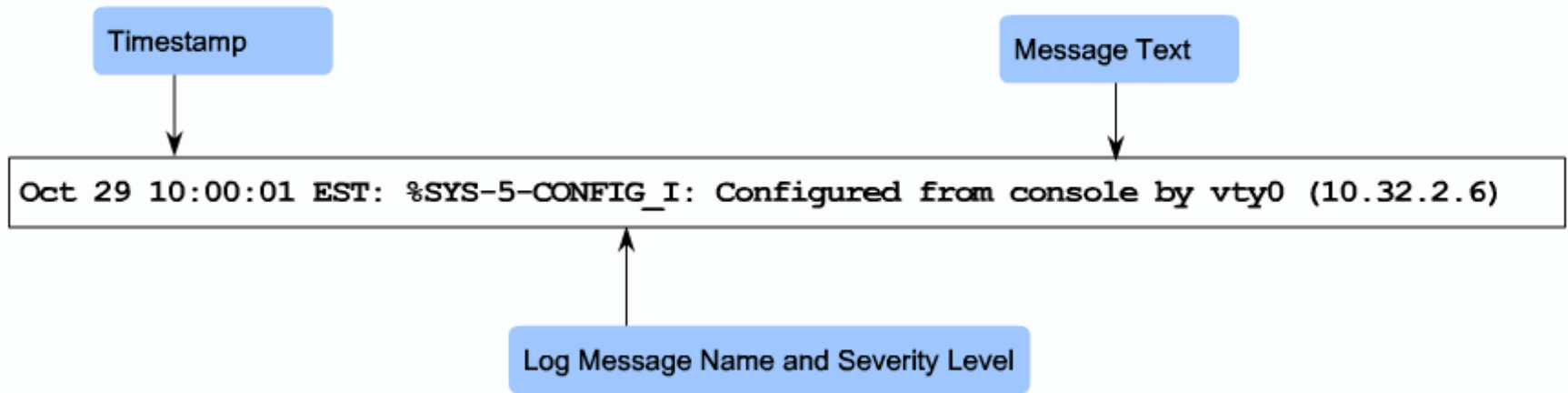
SNMP levels of security

- ▶ The default community string is “public”
 - ▶ Many networks use this default value
 - ▶ Knowing the community string is like having the enable password for all the devices in the network
- ▶ SNMP v1 and v2 send their community string in clear text over the network
- ▶ If management is being done in-band anyone on the network can see the community string
- ▶ Devices should only be configured with a read-only community string
 - ▶ There will be no write access for network nodes

Network security and logging

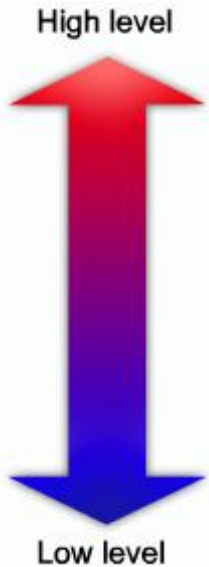
- ▶ Cisco routers can log information about most events that take place in the network
- ▶ Log messages can be sent to several logging facilities:
 - ▶ **Console**: this is on by default; log messages will appear automatically on the console over your command prompt
 - ▶ This is why you need to know the “logging synchronous” command 😊
 - ▶ **Terminal lines**: EXEC sessions from Telnet or SSH can also receive log messages
 - ▶ **Buffered logging**: log messages are stored in the router’s memory until reboot
 - ▶ **SNMP traps**: certain logged events can be forwarded as SNMP traps to a NMS
 - ▶ **Syslog**: log messages can be forwarded to an external syslog service; can be an application running on Windows or Linux

A sample log message



- ▶ Each log message has three fields:
 - ▶ A timestamp
 - ▶ The log message name and the severity level
 - ▶ The message text

Log message types



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

- ▶ Examples of events:
 - ▶ 0: IOS cannot load
 - ▶ 1: Temperature too high
 - ▶ 2: Unable to allocate memory
 - ▶ 3: Invalid memory size
 - ▶ 4: Crypto operation failed
 - ▶ 5: Interface changed state up or down
 - ▶ 6: Packet denied by ACL
 - ▶ 7: Packet type invalid

Network Time Protocol

- ▶ Clocks on network devices must be maintained and synchronized
- ▶ Misconfigured clocks can lead to:
 - ▶ Incorrect timestamps in system logs
 - ▶ Invalid time-based security certificates
 - ▶ Other time-related configurations
- ▶ The time and date can be set on Cisco routers
 - ▶ Manually (works, but don't expect any synchronization)
 - ▶ Does not scale well
 - ▶ Automatically, using NTP

Manually setting the clock

- ▶ This is how you manually set the clock:

```
R2#clock set 19:02:00 OCT 17 2009
```

```
R2#
```

```
*Oct 17 19:02:00.000: %SYS-6-CLOCKUPDATE: System clock has been  
updated from 00:05:26 UTC Fri Mar 1 2002 to 19:02:00 UTC Sat  
Oct 17 2009, configured from console by console.
```

- ▶ Notice the syslog message
- ▶ Also notice that this command is NOT entered in the configuration mode. Why?

NTP facts

- ▶ NTP allows routers on a network to synchronize their time settings with a time server
 - ▶ Obtaining the time from a single source provides more consistent time settings
- ▶ You can implement your own time server or you can even use a publicly available NTP server, from the Internet
- ▶ NTP works on UDP port 123

Securing NTP

- ▶ Getting time from the Internet is easy and can be accurate enough. But...
- ▶ Most time servers do not require any authentication
- ▶ An attacker can inject a false time value in your network
 - ▶ Possibly during an attack to make tracing difficult
 - ▶ Or to make digital certificates invalid and disrupt operations

Configuring basic NTP

- ▶ To make a router an NTP server:

```
R2(config)#ntp master 1
```

- ▶ The “1” represents the stratum number.
- ▶ The stratum number is the number of hops between the NTP server and authoritative source, such as an atomic clock.
- ▶ It basically says how trustworthy the time source is.
 - ▶ the lower, the better
- ▶ Then, configure the server’s address on the clients:

```
R1(config)#do sh clock
```

```
*00:11:08.955 UTC Fri Mar 1 2002
```

```
R1(config)#ntp server 10.0.0.2
```

```
R1(config)#do show clock
```

```
19:08:14.952 UTC Sat Oct 17 2009
```



Before



After

Verifying basic NTP

```
R1#show ntp status
```

```
Clock is synchronized, stratum 2, reference is 10.0.0.2  
nominal freq is 250.0000 Hz, actual freq is 249.9997 Hz,  
precision is 2**18  
reference time is CE84969D.9939A4FB (19:16:45.598 UTC Mon Oct 17  
2011)  
clock offset is -0.0892 msec, root delay is 3.94 msec  
root dispersion is 12.48 msec, peer dispersion is 12.36 msec
```

- ▶ Using the “ntp server” client command causes the clients to contact the server

- ▶ Servers can also broadcast their time settings on a LAN:

```
R2(config-if)#ntp broadcast destination 10.0.0.255
```

- ▶ And clients can listen for it:

```
R1(config-if)#ntp broadcast client
```

- ▶ Time accuracy is lower since communication is one-way only

Configuring secure NTP

- ▶ NTPv3 provides a cryptographic authentication mechanism between clients and the server
- ▶ NTPv3 uses keyed-MD5 authentication
- ▶ To configure NTP authentication, use the following commands on the server AND the clients:

```
R2 (config)#ntp authenticate
```

```
R2 (config)#ntp authentication-key 1 md5 CiscoTime
```

```
R2 (config)#ntp trusted-key 1
```

- ▶ Multiple keys can be defined, the “ntp trusted-key” command indicates which key will be used
- ▶ In addition, the clients must add:

```
R1 (config)#ntp server 10.0.0.2 key 1
```

- ▶ The server will still respond to unauthenticated requests

Verifying NTP authentication

- To check that NTP with authentication is used on clients:

```
R1#show ntp association detail
```

```
10.0.0.2 configured, authenticated, our_master, sane, valid, stratum 1
ref ID .LOCL., time CE849EC8.ABFD8D6E (19:51:36.671 UTC Sat Oct 17 2009)
our mode client, peer mode server, our poll intvl 256, peer poll intvl 256
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 8.347
delay 3.88 msec, offset 5.7161 msec, dispersion 6.38
precision 2**18, version 3
org time CE849ECF.1CB71019 (19:51:43.112 UTC Sat Oct 17 2009)
rcv time CE849ECF.1CAC9CDD (19:51:43.112 UTC Sat Oct 17 2009)
xmt time CE849ECF.1AAF3964 (19:51:43.104 UTC Sat Oct 17 2009)
filtdelay =      7.60      7.87      3.88      11.31      63.92      27.66      51.91      23.67
filtoffset =      3.96     -8.11      5.72      13.62      11.68      22.02       9.70      16.05
filtererror =      0.02      0.03      0.05      0.06      0.08      0.09      0.11      0.12
```

- Horrible. Let's try this:

```
R1#show ntp association detail | include 10.0.0.2
```

```
10.0.0.2 configured, authenticated, our_master, sane, valid, stratum 1
```

Better 😊

Auto-secure

- ▶ Cisco IOS provides an easy way to lock down your router in one step: the “auto secure” command
- ▶ Auto secure is a macro that will add the necessary commands to your running configuration file
- ▶ A wizard starts that queries the user for information

R1#auto secure

--- AutoSecure Configuration ---

***** AutoSecure configuration enhances the security of the router, but it will not make it absolutely resistant to all security attacks *****

...

AutoSecure lockdown

▶ AutoSecure the management plane

- ▶ BOOTP, CDP, FTP, TFTP, PAD, UDP and TCP small servers, MOP, ICMP, IP source routing, finger, password encryption, TCP keepalives, gratuitous ARP, proxy ARP, directed broadcast
- ▶ Configures a banner
- ▶ Secures passwords and login functions
- ▶ Secures NTP
- ▶ Secures SSH access
- ▶ TCP Intercept services

▶ AutoSecure the data plane

- ▶ Enable Cisco firewall inspection
- ▶ Enables traffic filtering using access lists
- ▶ Enables Cisco Express Forwarding (CEF)

AutoSecure modes

- ▶ The AutoSecure setup can run in an interactive mode:

`Router#auto secure`

- ▶ Or in a non-interactive mode (user is not asked):

`Router#auto secure no-interact`

```
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```

Parameter	Description
no-interact	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
full	(Optional) The user will be prompted for all interactive questions. This is the default setting.
forwarding	(Optional) Only the forwarding plane will be secured.
management	(Optional) Only the management plane will be secured.
ntp	(Optional) Specifies the configuration of the Network Time Protocol (NTP) feature in the AutoSecure command-line interface (CLI).
login	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
ssh	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
firewall	(Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI.
tcp-intercept	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

The quote means it's over 😊

“Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench.”

Gene Spafford