IOS Security

- When a Cisco router or switch is received from the factory no security is configured
- You can access the command line via a console cable with no password required
- One of the first tasks is to configure security to ensure that only authorised administrators can access the device

Basic Line Level Security

- Minimal password security can be configured through the use of static, locally defined passwords at three different levels:
    - Console line – accessing User Exec mode when connecting via a console cable
    - Virtual terminal VTY line – accessing User Exec mode when connecting remotely via Telnet or SSH Secure Shell
    - Privileged Exec Mode – entering the ‘enable’ command

- The levels can be used independently or in combination with each other.
- They can use the same or different passwords.

Basic Console Security

- Only one administrator can connect over a console cable at a time so the line number is always 0.
- ‘Login’ with no following keywords requires the administrator to enter the password configured at the line level to log in

    - *R1(config)#line console 0*
    - *R1(config-line)#password Flackbox1*
    - *R1(config-line)#login*

Basic Telnet Security

- An administrator can use Telnet to connect to the CLI of a router or switch remotely over an IP connection

- IOS devices do not accept incoming Telnet sessions by default
- An IP address and virtual terminal VTY line access must be configured

- Multiple administrators can connect at the same time. Lines are allocated on a first come first served basis
- If all configured lines are in use then additional administrators will not be able to login

R1(config)#line vty 0 15
R1(config-line)#password Flackbox2
R1(config-line)#login

Switch Management IP Address

- A Layer 2 Switch is not IP routing aware
- It does however support a single IP address for management
- A default gateway also needs to be configured to allow connectivity to other subnets

Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.0.1

Exec Timeout

- An administrator will be logged out after 10 minutes of inactivity by default. This applies to both the console and VTY lines
- You can edit this value with the exec-timeout command
- *no exec-timeout* or *exec-timeout 0* allows an administrator to stay logged in indefinitely

R1(config)#line con 0
R1(config-line)#exec-timeout 15
R1(config)#line vty 0 15
R1(config-line)#exec-timeout 5 30

Securing VTY Lines with Access Lists

- You can apply an Access List to control access to the VTY lines
- This can be used to limit Telnet and SSH access to only your administrator workstations

R1(config)#access-list 1 permit host 10.0.0.10
R1(config)#line vty 0 15
R1(config-line)#login
R1(config-line)#password Flackbox3
R1(config-line)#access-class 1 in

Basic Privileged Exec Security

- When you connect over the console or a VTY line you will land at the User Exec prompt which has a very limited set of commands available
- To get superuser access you use the ‘enable’ command to invoke Privileged Exec mode
- This can be secured with a password
- Disadvantage: enable password can be viewed in the show run config

R1(config)#enable password Flackbox3

Enable Secret

- An enable secret performs the same function as the enable password
- The enable secret is always shown in an encrypted format in the running configuration
- If both an enable password and enable secret are configured, the enable secret supersedes the enable password which is no longer used
- Best practice is to configure an enable secret but not an enable password

Encrypting Passwords

Line level passwords can also be viewed in plain text in the running configuration by default.

```
R1#show run
!
enable secret 5 $1$mERr$ABB9Y2FkwbWuPLfUgLUxf1
enable password Flackbox3
!
line con 0
password Flackbox1
login
!
line vty 0 4
password Flackbox2
login
line vty 5 15
password Flackbox2
login
```

Service Password-Encryption

- The service password encryption command encrypts all passwords in the running configuration
- It is best practice to enable this

R1(config)#service password-encryption

```
R1#show run
!
service password-encryption
!
enable secret 5 $1$mERr$ABB9Y2FkwbWuPLfUgLUxf1
enable password 7 0807404F0A1207180A58
!
line con 0
password 7 0807404F0A1207180A5A
login
!
line vty 0 4
password 7 0807404F0A1207180A59
login
line vty 5 15
password 7 0807404F0A1207180A59
login
```

Username Level Security

- More granular security can be provided by configuring individual usernames and passwords for different administrators

R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 secret Flackbox2
R1(config)#line console 0
R1(config-line)#login local (use local usernames)
R1(config)#line vty 0 15
R1(config-line)#login local

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Username: admin1
Password: <Flackbox1>
R1>
```

Privilege Levels

- There are 16 privilege levels of admin access (0-15) available on a Cisco router or switch
- Usernames can be assigned a privilege level. The default level is 1.
- You can also configure different passwords for direct access to the different privilege levels
- Each available command in IOS can be assigned a privilege level. An administrator must be logged in with that privilege level or higher to run the command

- By default, three levels of privilege are used - zero, user, and privileged. All commands are at one of these three levels by default
- Zero-level access allows only five commands—logout, enable, disable, help, and exit.
- User level (level 1) provides very limited read-only access to the router. When you enter User Exec Mode you're at Privilege Level 1 by default
- Privileged level (level 15) provides complete control over the router. When you enter Privileged Exec Mode with the 'enable' command you're at Level 15 by default

R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 privilege 15 secret Flackbox2
R1(config)#line console 0
R1(config-line)#login local
R1(config)#line vty 0 15
R1(config-line)#login local

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Username: admin1
Password: <Flackbox1>
R1>
R1>show privilege
Current privilege level is 1
```

Configuring Command Privilege Levels Example

Only admin2 has *superuser* privileges
R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 privilege 15 secret Flackbox2
R1(config)#username admin3 privilege 5 secret Flackbox3

Change command privilege level. Now also admin3 can execute *show run conf*
R1(config)#privilege exec level 5 show running-config

R1(config)#enable secret secret1 (sets password for privilege level 15)
R1(config)#enable secret level 5 secret2 (sets password for privilege level 5)

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open
User Access Verification
Username: admin1
Password: <Flackbox1>

R1>show run
^
% Invalid input detected at '^' marker.

R1>enable 5
Password: <secret2>
R1#show run
Building configuration...


Current configuration : 1380 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
```

Telnet vs SSH

- All Telnet communications cross the network in plain text
- If somebody sniffs the traffic using a tool such as Wireshark they can see all the commands you enter including your username and password
- All SSH Secure Shell traffic is encrypted
- If somebody sniffs the traffic they cannot read it
- Best practice is to disable Telnet and only allow SSH for administrator CLI access

Enable SSH

- A digital certificate with a key length of at least 768 bits must be generated to enable SSH encryption

```
R1(config)#ip domain-name flackbox.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.flackbox.com
Choose the size of the key modulus in the range of 360 to 2048
for your General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-
exportable...[OK]
```

Disable Telnet

- VTY lines are used for both Telnet and SSH connections
- Access is allowed for both by default
- A username is required for SSH access (line level passwords are not supported)

R1(config)#username Flackbox secret Flackbox1
R1(config)#line vty 0 15
R1(config-line)#transport input ssh (telnet not added)
R1(config-line)#login local (use local usernames)
R1(config-line)#exit
R1(config)#ip ssh version 2 (limit SSH to v2)

AAA Server

- Configuring line level security or local usernames on each device has a serious scalability limitation
- If a password has to be added, changed or removed it needs to be done on all devices
- An external AAA server can be used to centralise this instead
- Multiple AAA servers can be implemented for redundancy

- AAA servers provide Authentication, Authorization and Accounting.
- Authentication verifies somebody is who they say they are. This is most commonly achieved with a username and password.
- Authorization specifies what a particular user is allowed to do, such as running a particular command.
- Accounting keeps track of the actions a user has carried out.
- Authorization and Accounting are optional. Authentication is mandatory if Authorization and/or Accounting are used.

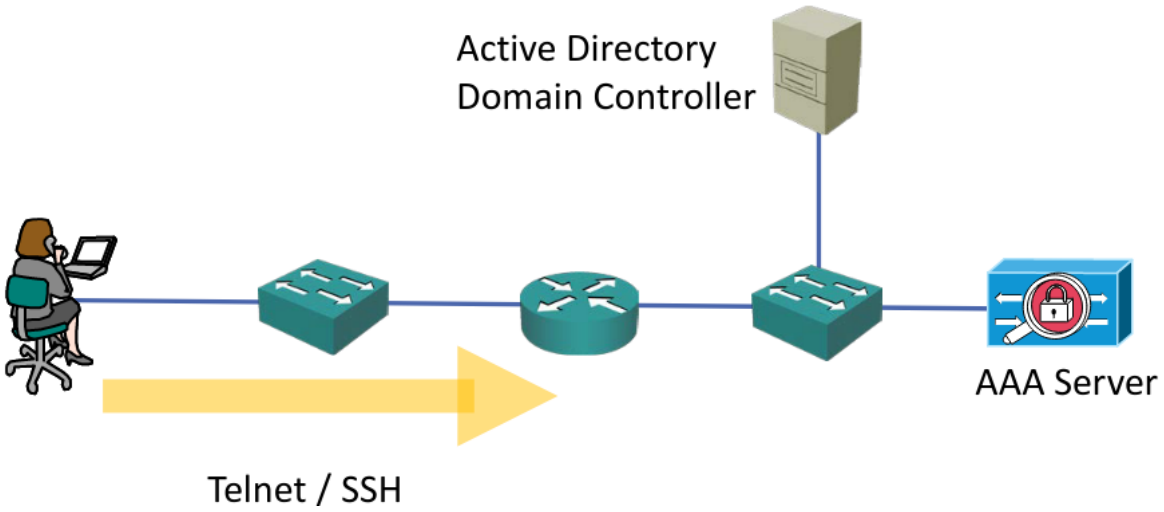
RADIUS and TACACS+

- The protocols which are used for AAA services are RADIUS and TACACS+
- Both are open standards, although vendors may add their own proprietary extensions
- Many vendor's AAA servers support both protocols
- RADIUS is commonly used for end user level services, such as VPN access
- TACACS+ is commonly used for administrator access on Cisco devices as it has more granular authorization capabilities

Cisco AAA Servers

- Cisco's AAA server is the Identity Services Engine (ISE)
- They also offered the Access Control Server (ACS) for a long time but it is now end of sale

Active Directory Integration



RADIUS/TACACS+ Configuration

Old RADIUS Configuration

R1(config)#username BackupAdmin secret Flackbox1 (configure a local user in case connectivity to the AAA server is lost)

R1(config)#aaa new-model

R1(config)#radius-server host 10.10.10.10 key Flackbox1
R1(config)#radius-server host 10.10.10.11 key Flackbox2

R1(config)#aaa group server radius FB-RG (optional)
R1(config-sg-radius)#server 10.10.10.10
R1(config-sg-radius)#server 10.10.10.11

R1(config)#aaa authentication login default group radius local
(Use all RADIUS servers) OR:
R1(config)#aaa authentication login default group FB-RG local
(Use servers in specified group)

New RADIUS Configuration

R1(config)#radius-server host 10.10.10.10
Warning: This CLI will be deprecated soon. Please move to radius server <name> CLI.

R1(config)#aaa new-model

R1(config)#radius server Server1
R1(config-radius-server)# address ipv4 10.10.10.10
R1(config-radius-server)# key Flackbox1

R1(config)#radius server Server2
R1(config-radius-server)# address ipv4 10.10.10.11
R1(config-radius-server)# key Flackbox2

R1(config-radius-server)#aaa group server radius FB-RG
R1(config-sg-radius)# server name Server1
R1(config-sg-radius)# server name Server2

R1(config-sg-radius)#aaa authentication login default group FB-RG local

Old TACACS+ Configuration

R1(config)#username BackupAdmin secret Flackbox1

R1(config)#aaa new-model

R1(config)#tacacs-server host 10.10.10.10 key Flackbox1
R1(config)#tacacs-server host 10.10.10.11 key Flackbox2

R1(config)#aaa group server tacacs+ FB-TG
R1(config-sg-tacacs+)#server 10.10.10.10
R1(config-sg-tacacs+)#server 10.10.10.11

R1(config)#aaa authentication login default group FB-TG local

New TACACS+ Configuration

R1(config)#tacacs-server host 10.10.10.10
Warning: This CLI will be deprecated soon. Please move to tacacs server <name> CLI.

R1(config)#username BackupAdmin secret Flackbox1

R1(config)#aaa new-model
R1(config)#tacacs server Server1
R1(config-server-tacacs)# address ipv4 10.10.10.10
R1(config-server-tacacs)# key Flackbox1

R1(config)#tacacs server Server2
R1(config-server-tacacs)# address ipv4 10.10.10.11
R1(config-server-tacacs)# key Flackbox2

R1(config-radius-server)#aaa group server tacacs+ FB-TG
R1(config-sg-tacacs+)# server name Server1
R1(config-sg-tacacs+)# server name Server2

R1(config-sg-tacacs+)#aaa authentication login default group FB-TG local

Best Practices

Login and Exec Banners

- Messages can be displayed in the CLI before and/or after an administrator logs in to a Cisco IOS device
- This is most commonly used to display security warnings

```
R1(config)#banner login ‟ (hit enter here)
Enter TEXT message. End with the character '"'.
Authorized users only‟

R1(config)#banner exec "
Enter TEXT message. End with the character '"'.
Please log out immediately if you are not an authorized
administrator"
```

```
C:\> telnet 10.0.0.1
Trying 10.0.0.1 …Open

Authorized users only

User Access Verification
Password: Flackbox3
Please log out immediately if you are not an authorized administrator
R1>enable
```

Disable Unused Services

- It is best practice to disable unused services
- This reduces the attack surface and also the load on the device
- HTTPS is sometimes used by GUI administration tools but HTTP should be disabled
- CDP should also be disabled in highly secure environments

R1(config)#no ip http server
R1(config)#no cdp run

Time Synchronisation - NTP

- All servers and infrastructure devices in your network should be synchronised to the same time
- This aids in troubleshooting as logs will report the correct time that events occurred
- It is also required by several security features such as Kerberos authentication and digital certificates

NTP Network Time Protocol

- Servers and infrastructure devices can use their own internal clock or synchronise with an external NTP server
- An NTP server should be used to ensure all devices have the same time
- A Cisco router can function as an NTP server and/or client

```
R1(config)#clock timezone PST -8
R1(config)#ntp server 10.0.1.100 (configures router to be NTP client)
R1(config)#ntp master (configures router to be NTP server)

R1#show clock
16:19:36.51 PST Mon Oct 2 2017

R1#show ntp status
Clock is synchronized, stratum 2, reference is 10.0.1.100
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is DD53255C.0000039C (00:16:28.924 UTC Tue Jan 2 2018)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```

Syslog

- Logging messages on Cisco devices comply with the Syslog standard
- A Syslog message is generated when something happens on the device, such as an interface going down or an OSPF neighbour adjacency coming up

Syslog Format

The format of the messages is:
seq no:time stamp: %facility-severity-MNEMONIC:description

Example:
*Oct 3 00:44:12.627: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down

Syslog Severity Levels

Value	Severity	Description
0	Emergency	System is unusable. A panic condition.
1	Alert	A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	Critical conditions, such as hard device errors.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Not errors, but may require special handling.
6	Informational	Informational messages.
7	Debug	Messages that contain information normally of use only when debugging a program.

Logging Locations

- Syslog messages can be logged to various locations:
    - **Console line** - events will be shown in the CLI when you are logged in over a console connection. All events logged by default
    - **VTY Terminal line**s - events will be shown in the CLI when you are logged in over a Telnet or SSH session. Not enabled by default
    - **The logging buffer** – events saved in RAM memory, you can view them with the 'show logging' command. All events logged by default
    - **External Syslog servers**

- You can specify the same or different severity levels to log for each location
- All messages of that severity level and higher will be logged
- For example, if you set a logging level of 3 for the console, events with severity levels 0, 1, 2 and 3 will be logged there
- If you set a logging level of 7 for an external Syslog server, events from all severity levels 0–7 will be logged there

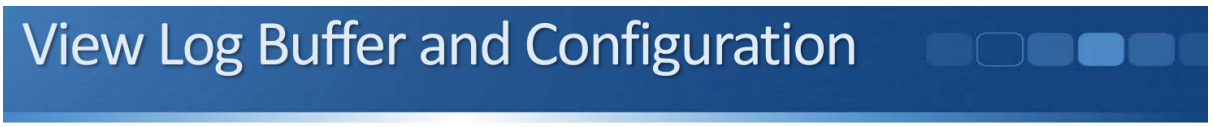
Internal Logging Locations Configuration

- *R1(config)#no logging console* (disables logging to the console line)
- *R1(config)#logging monitor 6* (events with severity level informational and higher will be logged to the VTY lines)

- *R1(config)#logging buffered debugging* (events with severity level 7 and higher will be logged to the buffer)

Logging to an External Syslog Server

- You can log to an external Syslog server to centralise event reporting
- You will typically set verbose logging to provide detailed troubleshooting information
- *R1(config)#logging 10.0.0.100*
- *R1(config)#logging trap debugging*




```
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns,
xml disabled, filtering disabled)

    Console logging: level error, 42 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level warning, 38 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 87 messages logged, xml disabled,
                    filtering disabled

    Trap logging: level debugging, 27 message lines logged
        Logging to 10.0.0.100  (udp port 514, audit disabled,
              link up),

Log Buffer (8192 bytes):

*Nov 12 21:17:08.015: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table No such
file or directory
*Nov 12 21:17:08.299: %DEC21140-1-INITFAIL: Unsupported PHY brand timed out, csr5=0x0
*Nov 12 21:17:14.075: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Nov 12 21:17:14.115: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
```

Logging Synchronous

- When working in a CLI session, by default any syslog messages will be printed into the middle of any commands you are currently typing

```
R1(config)#interface f3/0
R1(config-if)#shutdown
R1(config-if)#do show ip interf
*Nov 12 20:27:00.727: %LINK-5-CHANGED: Interface
FastEthernet3/0, changed state to administratively downace br
```

- You can override this with the logging synchronous command
- This causes a new line to be printed where you were in the command

```
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#interface f3/0
R1(config-if)#no shutdown
R1(config-if)#do show ip interf
*Nov 12 20:29:48.787: %LINK-3-UPDOWN:
Interface FastEthernet3/0, changed state to up
R1(config-if)#do show ip interf
```

Debug and Terminal Monitor

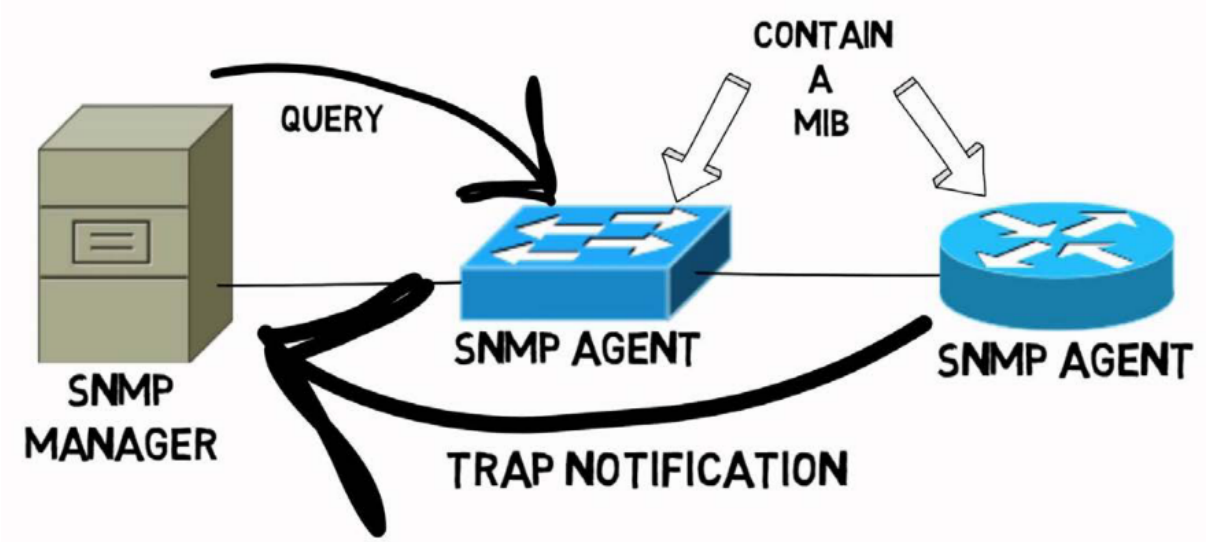
- Show and Debug commands can be used to view specific information over and above the standard Syslog messages
- Show output shows a static point in time state
- Debug output dynamically updates in real time
- Be careful with debug commands in production environments, a large amount of output can overwhelm the device
- Debug output is logged to the console line and buffer by default
- Use the R1#terminal monitor command to enable debug output to the VTY lines

Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP) is an open standard for network monitoring.
- An SNMP Manager (the SNMP server) can collect and organize information from an SNMP Agent, which is SNMP software which runs on managed devices such as routers and switches.
- The SNMP Manager is commonly called an SNMP Server or NMS (Network Management System).
- The SNMP Manager can pull information from the device (‘Get’) or the device can push it to the server (‘Trap’).
- For example the Manager could query traffic statistics from the device or the device could report an HSRP state change.
- The standard also includes support for modifying Agent information from the SNMP Manager to change device behaviour.

MIB Management Information Base

- Data variables on SNMP managed systems are organized in a Management Information Base (MIB).
- The SNMP Manager and Agent need to share the MIB so they know which variables can be reported on.



SNMP Versions

- Three significant versions of SNMP have been developed and deployed.
- SNMPv1 uses plain text authentication between the Manager and Agent using matching Community strings.
- SNMPv2c also uses plain text Community strings. It supports bulk retrieval.
- SNMPv3 supports strong authentication and encryption. It is the preferred version but is not supported on all devices.

SNMPv2c Community Strings

- SNMPv2c uses Community strings rather than a username and password to authenticate the SNMP Manager and Agent to each other
- Matching community strings need to be set on both sides for the Manager and Agent to communicate
- The read only (ro) community is used by the Manager to read information
- The read write (rw) community is used by the Manager to set information

SNMPv2 Configuration


```
R1(config)#snmp-server contact neil@flackbox.com
R1(config)#snmp-server location Flackbox Lab
```

(Optional, identifies the Agent to the Manager)

```
R1(config)#snmp-server community Flackbox1 ro
R1(config)#snmp-server community Flackbox2 rw

R1(config)#snmp-server host 10.0.0.100 Flackbox1
R1(config)#snmp-server enable traps config
```

(When a configuration change is made a trap will be sent to the NMS system at 10.0.0.100 using the ro Community string)

SNMPv3 Configuration

- The SNMP Manager and Agent recognise each other through simple unencrypted community strings in SNMP version 1 and 2
- SNMPv3 supports authentication and encryption
- The SNMPv3 security model works with users and groups
- A matching user account is set up on the NMS server and network device
- Settings are derived from the group the user is a member of

SNMPv3 Security Levels

- 3 different security levels are available. They are configured at the group level:
    - noAuthnoPriv - no authentication password is exchanged and the communications between the agent and the server are not encrypted. The username serves as replacement for community string.
    - AuthNoPriv - Password authentication is used. No encryption is used for communications between the devices.
    - AuthPriv - Password authentication is used. Communications between the agent and the server are also encrypted.

```
R1(config)#snmp-server group Flackbox-group v3 ?
  auth     group using the authNoPriv Security Level
  noauth   group using the noAuthNoPriv Security Level
  priv     group using SNMPv3 authPriv security level

R1(config)#snmp-server group Flackbox-group v3 priv ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the group
  match    context name match criteria
  notify   specify a notify view for the group
  read     specify a read view for the group
  write    specify a write view for the group
  <cr>
```

SNMPv3 Configuration - Group

- **Access** can be used to reference an access-list which limits the device to communicating with the IP address of the NMS server only
- **Contexts** are used on switches to specify which VLANs are accessible via SNMP

SNMPv3 Configuration - Views

- Views can be used to limit what information is accessible to the NMS server.
- If you don't specify a read view then **all** MIB objects are accessible to read.
- If you don't specify a write view then **no** MIB objects are accessible to write.
- The NMS server gets read only access to all MIBs by default.
- The notify view is used to send notifications to members of the group. If you don't specify any then it will be disabled by default.

SNMPv3 Configuration - Group

```
R1(config)#snmp-server group Flackbox-group v3 priv
```

SNMPv3 Configuration - User

```
R1(config)#snmp-server user Flackbox-user Flackbox-group v3 auth ?
  md5  Use HMAC MD5 algorithm for authentication
  sha  Use HMAC SHA algorithm for authentication
```
(most secure but slower)

SNMPv3 Configuration - User

```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv ?
  3des  Use 168 bit 3DES algorithm for encryption
  aes   Use AES algorithm for encryption (most secure but slower)
  des   Use 56 bit DES algorithm for encryption
```

SNMPv3 Configuration - User

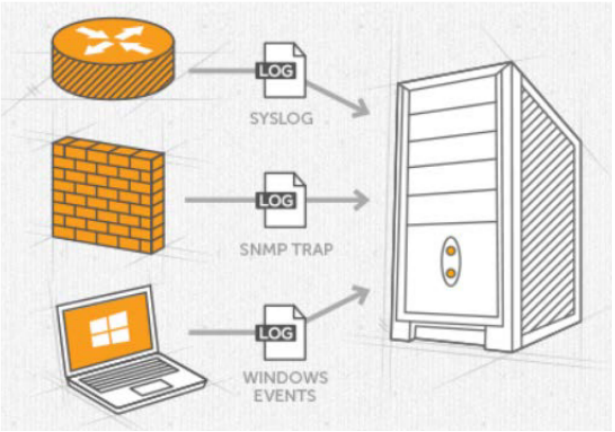
```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv aes ?
  128  Use 128 bit AES algorithm for encryption
  192  Use 192 bit AES algorithm for encryption
  256  Use 256 bit AES algorithm for encryption
```

SNMPv3 Configuration - User

```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv aes 128 PRIVPASSWORD
```

Syslog vs SNMP

- Both Syslog and SNMP provide logging functionality.
- Syslog can often provide more granular detail than SNMP but it has support for the device pushing information only (not pulling or setting from the server).
- NMS servers will typically support both Syslog and SNMP



NMS vs SIEM

- There is some overlap between NMS and SIEM products. Both can gather logging information from network infrastructure devices such as routers, switches and firewalls using protocols such as Syslog, SNMP and NetFlow.
- A product which is marketed as an NMS will have a focus on collating network information and provide reports, early warning of and easier troubleshooting of network events.
- A product which is marketed as a SIEM will have a focus on collating security information and provide reports, early warning of and easier troubleshooting of security events.