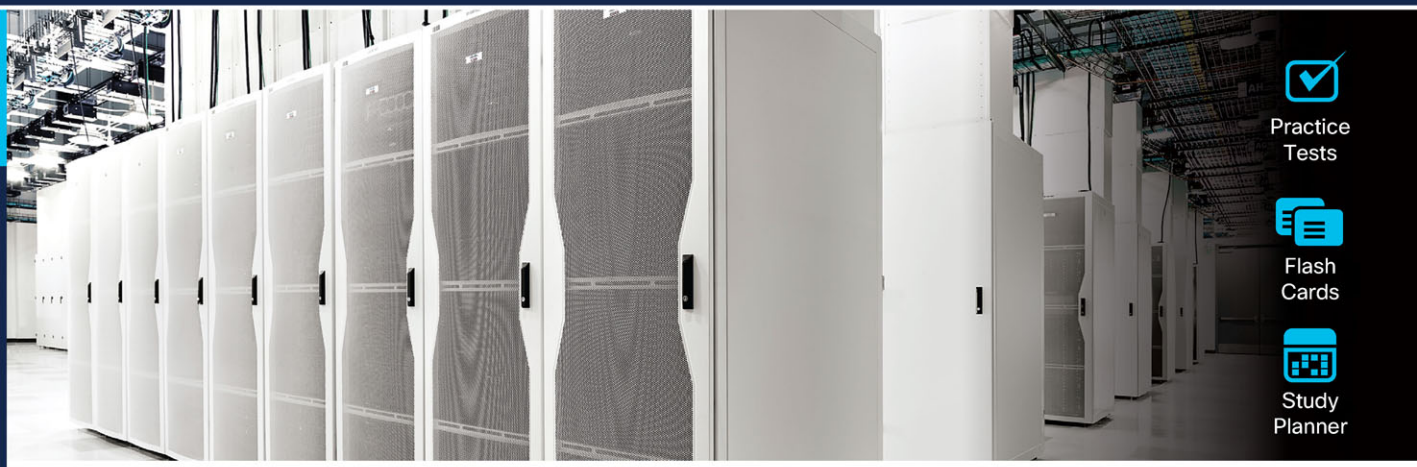
Official Cert Guide



Review Exercises

CCNP and CCIE Data Center Core

DCCOR 350-601

2nd Edition

Somit Maloo
CCDE® No. 20170002, CCIE® No. 28603
Iskren Nikolov
CCIE® No. 20164, CCNP Data Center, CCSI® No. 32481
Firas Ahmed
CCIE® No. 14967

ciscopress.com

CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the print book ISBN: **9780138228088**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- **noAuthNoPriv:** Security level that does not provide authentication or encryption. This level is not supported for SNMPv3.
- **authNoPriv:** Security level that provides authentication but does not provide encryption.
- **authPriv:** Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determines the security mechanism applied when the SNMP message is processed. Table 6-11 identifies what the combinations of security models and levels mean.

Key Topic

Table 6-11 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) message digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

Tables 6-12 through 6-15 describe the most-used SNMP configuration commands. For a full list of the commands, refer to the Nexus System Management Configuration Guide links shown in the reference list at the end of this chapter.

Table 6-12 SNMP Global Commands

Command	Purpose
snmp-server *user name* [**auth** { **md5** | **sha** } **passphrase** [**auto**] [**priv** [**aes-128**] **passphrase**] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters. The passphrase can be any case-sensitive alphanumeric string up to 64 characters. If you use the **localizedkey** keyword, the passphrase can be any case-sensitive alphanumeric string up to 130 characters. The **engineID** format is a 12-digit colon-separated decimal number.

Command	Purpose
snmp-server *user name* **enforcePriv**	Enforces SNMP message encryption for this user.
snmp-server *user name group*	Associates this SNMP user with the configured user role.
snmp-server community *name group* { **ro** | **rw** }	Creates an SNMP community string.
snmp-server community *community-name* **use-acl** *acl-name*	Assigns an ACL to an SNMP community to filter SNMP requests.
snmp-server host *ip-address* { **traps** | **informs** } **version 2c** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 or IPv6 address. The *community* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65,535.
snmp-server host *ip-address* { **traps** | **informs** } **version 3** { **auth** | **noauth** | **priv** } *username* [**udp_port** *number*]	Configures a host receiver for SNMPv3 traps or informs. The *ip-address* can be an IPv4 or IPv6 address. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65,535.
snmp-server host *ip-address* **source-interface if-type if-number** [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 or IPv6 address. Use **?** to determine the supported interface types. The UDP port number range is from 0 to 65,535. This configuration overrides the global source interface configuration.
snmp-server source-interface { **traps** | **informs** } **if-type if-number**	Configures a source interface for sending out SNMPv2c traps or informs. Use **?** to determine the supported interface types.

Table 6-13 SNMP MIBs

MIB	Purpose
All notifications	snmp-server enable traps
CISCO-AAA-SERVER-MIB	snmp-server enable traps aaa snmp-server enable traps aaa server-state-change
CISCO-BGP4-MIB	snmp-server enable traps bgp
CISCO-STP-BRIDGE-MIB	snmp-server enable traps bridge snmp-server enable traps bridge newroot snmp-server enable traps bridge topologychange
CISCO-CALLHOME-MIB	snmp-server enable traps callhome snmp-server enable traps callhome event-notify snmp-server enable traps callhome smtp-send-fail
CISCO-CFS-MIB	snmp-server enable traps cfs snmp-server enable traps cfs merge-failure snmp-server enable traps cfs state-change-notif

MIB	Purpose
CISCO-CONFIG-MAN-MIB	snmp-server enable traps config snmp-server enable traps config ccmCLIRunningConfigChanged
CISCO-EIGRP-MIB	snmp-server enable traps eigrp [*tag*]
ENTITY-MIB, CISCO-ENTITY- SENSOR-MIB	snmp-server enable traps entity snmp-server enable traps entity entity_fan_status_change snmp-server enable traps entity entity_mib_change snmp-server enable traps entity entity_module_inserted snmp-server enable traps entity entity_module_removed snmp-server enable traps entity entity_module_status_change snmp-server enable traps entity entity_power_out_change snmp-server enable traps entity entity_power_status_change snmp-server enable traps entity entity_unrecognised_module
CISCO-FEATURE- CONTROL-MIB	snmp-server enable traps feature-control snmp-server enable traps feature-control FeatureOpStatusChange
CISCO-HSRP-MIB	snmp-server enable traps hsrp snmp-server enable traps hsrp state-change
CISCO-LICENSE-MGR-MIB	snmp-server enable traps license snmp-server enable traps license notify-license-expiry snmp-server enable traps license notify-license-expiry-warning snmp-server enable traps license notify-licensefile-missing snmp-server enable traps license notify-no-license-for-feature
IF-MIB	snmp-server enable traps link snmp-server enable traps link IETF-extended-linkDown snmp-server enable traps link IETF-extended-linkUp snmp-server enable traps link cisco-extended-linkDown snmp-server enable traps link cisco-extended-linkUp snmp-server enable traps link linkDown snmp-server enable traps linkUp
OSPF-MIB, OSPF-TRAP-MIB	snmp-server enable traps ospf [*tag*] snmp-server enable traps ospf lsa snmp-server enable traps ospf rate-limit *rate*

MIB	Purpose
CISCO-PORT-SECURITY-MIB	snmp-server enable traps port-security snmp-server enable traps port-security access-secure-mac-violation snmp-server enable traps port-security trunk-secure-mac-violation
CISCO-RF-MIB	snmp-server enable traps rf snmp-server enable traps rf redundancy_framework
CISCO-RMON-MIB	snmp-server enable traps rmon snmp-server enable traps rmon fallingAlarm snmp-server enable traps rmon hcFallingAlarm snmp-server enable traps rmon hcRisingAlarm snmp-server enable traps rmon risingAlarm
SNMPv2-MIB	snmp-server enable traps snmp snmp-server enable traps snmp authentication

Table 6-14 SNMP Specific Notification Commands

Command	Purpose
snmp-server enable traps	Enables all SNMP notifications.
snmp-server enable traps aaa [server-state-change]	Enables AAA SNMP notifications. Optionally, enables the following specific notifications: **server-state-change:** Enables AAA server state-change notifications.
snmp-server enable traps bgp	Enables BGP SNMP notifications.
snmp-server enable traps callhome [event-notify]	Enables Call Home notifications. Optionally, enables the following specific notifications: **event-notify:** Enables Call Home external event notifications. **smtp-send-fail:** Enables Simple Mail Transfer Protocol (SMTP) message send fail notifications.
snmp-server enable traps snmp [authentication]	Enables general SNMP notifications. Optionally, enables the following specific notification: **authentication:** Enables SNMP authentication notifications.

Table 6-15 SNMP Verification Commands

Command	Purpose
show interface snmp-ifindex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.

Command	Purpose
show snmp group	Displays SNMP roles.
show snmp host	Displays information about configured SNMP hosts.
show snmp session	Displays SNMP sessions.
show interface snmp-ifindex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show running-config snmp [all]	Displays the SNMP running configuration.

Example 6-6 shows how to configure Cisco NX-OS to send the Cisco link Up or Down notifications to a notification host receiver using the Blue VRF and defines two SNMP users—Admin and NMS.

Example 6-6 *NX-OS SNMP Configuration Example*

```
switch# config t
switch(config)# snmp-server contact Admin@company.com
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:
   00:63:00:01:00:22:32:15:10:03
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
switch(config)# snmp-server enable traps link cisco
```

Example 6-7 shows how to configure SNMP to send traps using an in-band port configured at the host level.

Example 6-7 *NX-OS SNMP Destination Trap Server and Source Interface Configuration*

```
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
```

Example 6-8 shows SNMP verification that shows the destination host with the SNMP version.

Example 6-8 *NX-OS SNMP Status*

```
switch(config)# show snmp host
-------------------------------------------------------------------
Host            Port  Version  Level   Type  SecName
-------------------------------------------------------------------
171.71.48.164   162   v2c      noauth  trap  public
 Source interface: Ethernet 1/2
-------------------------------------------------------------------
```

Nexus Smart Call Home

Smart Call Home provides an email-based notification for critical system policies. A range of message formats is available for compatibility with pager services, standard email, or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a network operations center, or use Cisco Smart Call Home services to automatically generate a case with the Cisco Technical Assistance Center.

Smart Call Home offers the following features:

- Automatic execution and attachment of relevant CLI command output.
- Multiple message format options such as the following:
  - **Short text:** Suitable for pagers or printed reports.
  - **Full text:** Fully formatted message information suitable for human reading.
  - **XML:** Machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML Schema Definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Cisco Technical Assistance Center.
- Multiple concurrent message destinations. You can configure up to 50 email destination addresses for each destination profile.

Example 6-9 shows how to configure Smart Call Home to send alerts via email when users configure a new routing protocol using the **show ip routing** command.

Example 6-9 *NX-OS Call Home Configuration Example*

```
switch(config)# snmp-server contact person@company.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# destination-profile Noc101 full-text
switch(config-callhome)# destination-profile full-text-destination email-addr
    person@company.com
switch(config-callhome)# destination-profile full-text-destination message-level 5
switch(config-callhome)# destination-profile Noc101 alert-group Configuration
switch(config-callhome)# alert-group Configuration user-def-cmd "show ip routing"
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# enable
switch(config-callhome)# commit
```


Key Topic

Nexus NetFlow

Today data center administrators need detailed profiles of applications that traverse their networks. To efficiently operate, scale, and consolidate their networks, administrators need to know what applications are consuming bandwidth, who is using them, when they are being used, and what activities are prevalent in the data center. With this information, data center administrators have visibility into their networks, which is crucial in exerting control over the network, finding the precise reasons for performance problems and possible security concerns, and managing the overall end-user experience.

The capability to characterize IP traffic and understand who sent it, the traffic destination, the time of day, and the application information is critical for data center operations. It helps data center managers determine how to optimize resource utilization, plan network capacity, build traffic pattern models for consolidation, and determine where to apply quality of service (QoS), and it plays a vital role in network security for detection of DoS attacks and network-propagated worms (see Figure 6-8).