Operations Alert Bulletin

Correcting QAM, MQAM, GQAM, or GoQAM Modulators With Missing Key Certificates

Purpose

This alert bulletin informs DNCS operators and engineers of a potential issue with the addition or replacement of QAM, MQAM, GQAM or GoQAM modulators to their network. If encrypted sessions are requested from a modulator having a missing key certificate on the DNCS, then each request fails. Additionally, digital video recorder (DVR) units *may* not be able to record and play back content provided by a QAM modulator that is missing a key certificate.

This bulletin provides instructions for using a script to proactively determine whether a modulator has a missing key certificate on the DNCS. Instructions are also provided to retrieve the missing key certificate in the event it is not stored in the DNCS.

Audience

This alert is written for Digital Network Control System (DNCS) operators and Cisco Services personnel who are familiar with a UNIX editor.

Background

If a modulator is added or replaced in a network, the DNCS may initially configure the key certificate as an invalid value, for example, 0 or NULL. Upon reboot of the modulator, its IP address is stored in the DNCS database; however, the key certificate is not correctly stored because a 0 or NULL value already exists in the database.

Unencrypted sessions can be built on modulators that have a 0 or NULL certificate. As a result, this condition can go unnoticed. Encrypted sessions, however, cannot be built on these modulators unless the correct certificate is known by the DNCS.

Whenever modulators are added or replaced in the network, the procedures within the **Recommendations** section of this Operations Alert Bulletin must be followed. This ensures that the key certificate for the new modulator is correctly stored on the DNCS.

Recommendations

DNCS operators should complete the process provided in this bulletin each time a modulator is added or replaced in the network.

Note: This process only needs to be performed once to correct any underlying problems. Perform this process again whenever a modulator is added or replaced in the network.

1. Retrieve the checkQamCert.sh script.
2. Install the checkQamCert.sh script onto the DNCS.
3. Run the checkQamCert.sh script and evaluate the results of the script to determine if any modulators are missing key certificates within the DNCS database.
4. Retrieve the key certificate data for modulators missing the key certificate.

Retrieving the checkQamCert.sh Script

Complete the following steps to retrieve the checkQamCert.sh script from the Cisco corporate FTP site.

1. In the URL field of your Web browser, type **ftp://ftp.sciatl.com/** and then press **Enter**.

   Result: The FTP site window opens.

2. Right-click in the FTP window and select **Login As**.

   Result: The Log On As window opens.

3. In the User name field, type **anonymous**.
4. In the Password field, enter your email address.
5. Click **Log On**.
6. Navigate to the **/pub/scicare/TOOLS/scripts** folder.
7. Double-click the **checkQamCert.tar.gz** file.
8. Go to **Installing the checkQamCert.tar.gz Script on the DNCS**, next in this bulletin.

Installing the checkQamCert.tar.gz Script on the DNCS

Follow these steps to install the checkQamCert.tar.gz script onto the DNCS.

1. Copy the **checkQamCert.tar.gz** to the **export/home/doctor** folder onto your DNCS.
2. Open an xterm window, type **cd /export/home/doctor** and then press **Enter**.
3. Unzip the checkQamCert.tar.gz file by typing **gzip -d checkQamCert.tar.gz** and then pressing **Enter**.
4. Type **tar xvf checkQamCert.tar** and then press **Enter.**
5. Delete the **checkQamCert.tar** file.

   Result: The checkQamCert.sh file remains.
6. Go to **Running the checkQamCert.sh Script and Evaluating the Results**, next in this bulletin.

Correcting QAM, MQAM, GQAM, or GoQAM Modulators With Missing Key Certificates, Continued

Running the checkQamCert.sh Script and Evaluating the Results

Perform the following steps to run the checkQamCert.sh script and verify whether any modulators have key certificates missing from the DNCS database.

1. Type **checkQamCert.sh** to run the script.

   Result: A list of modulators appears *only* if their key certificates are missing from the DNCS database.

```
qam_id             42
ipaddr             172.16.4.37
qam_name           QAM14
mykeycert          4080442c0000000079fa7020
oidval             4080442c0000000079fa7020
certificatedata
datalen            0
distinguishedname  C=US;O=Cisco;CN=PK0002DE81F034
optimctrl          0

qam_id             35
ipaddr             172.16.4.51
qam_name           MQAM2
mykeycert          40741fe0000000079fa7020
oidval             40741fe0000000079fa7020
certificatedata
datalen            0
distinguishedname  C=US;O=Cisco;CN=PK0002DE8223A9
optimctrl          0
```

2. Review the list. Notice that the key certificate is missing for a QAM and an MQAM modulator because the **certificatedata** field is blank.

3. To retrieve the key certificate data for a modulator, go to **Retrieving Key Certificate Data for a Modulator**, next in this bulletin.

Retrieving Key Certificate Data for a Modulator

Complete the following process to allow the DNCS to retrieve the proper key certificates for the modulator.

Note: Performing this process requires you to reboot your session on the DNCS. Rebooting modulators on the DNCS interrupts active sessions; therefore, it is suggested that you *first* perform an auditQam to identify the number of active sessions. If you need assistance with this procedure, contact Cisco Services.

Special care should be taken with modulators carrying video-on-demand (VOD) and *anything*-On-Demand (xOD) programs that carry adult-oriented content. After the modulator reboots, a new program map table (PMT) is generated; however, some DHCTs may not have the ability to read the table. This causes the DHCT to display adult-rated content until encryption is reestablished, requiring some subscribers to tune off and back onto a program to regain the correct video.

Note: It is suggested that you reboot the modulator at off-peak hours to minimize the effect on subscriber services.

1. Click **Control** from the **DNCS** section of the DNCS Administrative Console Status window.

   Result: The DNCS Control window appears.

2. Select **camPSM** and then select **Stop Process** from the Process menu so that Entitlement Control Messages (ECMs) are not generated with the old key.

   Result: You are asked to confirm this request.

3. Click **Yes**.

4. Click **QAM** from the Element Provisioning section within the DNCS Administrative Console window.

   Result: The QAM List screen appears.

5. Select the *first* modulator in the list that is missing a key certificate.

6. Click **File** and then select **Open**.

   Result: The Set Up QAM window appears and displays the set up and connectivity for the modulator that you selected.

Correcting QAM, MQAM, GQAM, or GoQAM Modulators With Missing Key Certificates, Continued

7. Click **Save**.

   Result: The Set Up QAM window closes and the QAM List window appears in the forefront.

   Note: Only one modulator that is missing a key certificate will need to be saved.

8. Select the modulator that you just saved.

9. Click **File** and then select **Reset**.

   Result: You are asked to confirm whether or not you want to reset the QAM modulator.

10. Click **Yes**.

    Result: The modulator is forced to reboot, enabling the DNCS to retrieve the key certificate for the modulator.

11. Repeat steps 8 through 10 for each modulator that did not have a key certificate stored on the DNCS.

12. Select **camPSM** from the DNCS Control window and then select **Start Process**.

13. Go to **Retrieving the checkQamCert.sh Script**, earlier in this bulletin, and follow the instructions for missing key certificates.

    Result: If key certificates are still missing *after* re-running the checkQamCert.sh script, call Cisco Services.

Correcting QAM, MQAM, GQAM, or GoQAM Modulators With Missing Key Certificates, Continued

For More Information

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

July 2012 Printed in USA Part Number 745235 Rev C