DOCSIS 1.0 Baseline Privacy on the Cisco CMTS

Contents

Introduction

The main goal of Data-over-Cable Service Interface Specifications (DOCSIS) Baseline Privacy Interface (BPI) is to provide a simple data encryption scheme to protect data sent to and from cable modems in a Data over Cable network. Baseline privacy can also be used as a means to authenticate cable modems, and to authorize the transmission of multicast traffic to cable modems.

Cisco Cable Modem Termination System (CMTS) and cable modem products running Cisco IOS® Software images with a feature set including the characters "k1" or"k8" support Baseline privacy, for example ubr7200-k1p-mz.121-6.EC1.bin.

This document discusses Baseline privacy on Cisco products operating in DOCSIS1.0 mode.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on configuring a uBR7246VXR running Cisco IOS® Software Release 12.1(6)EC, but it also applies to all other Cisco CMTS products and software releases.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

How to Configure Baseline Privacy for Cable Modems

A Cable Modem will only attempt to use Baseline privacy if it is commanded to do so via the Class of service parameters in a DOCSIS configuration file. The DOCSIS configuration file contains operational parameters for the modem, and is downloaded through TFTP as part of the process of coming online.

One method of creating a DOCSIS configuration file is to use the DOCSIS Cable Modem Configurator on Cisco.com. Using the DOCSIS Cable Modem Configurator, you can create a DOCSIS configuration file that commands a Cable Modem to use Baseline Privacy by setting the Baseline Privacy Enable field under the Class of Service tab to **On**. Refer to the example below:

Alternatively, the standalone version of the DOCSIS file configuration from can be used to enable Baseline Privacy as shown below:

Once a DOCSIS configuration file supporting BPI has been created, cable modems will need to be reset in order to download the new configuration file and subsequently employ Baseline privacy.

How to Tell If a Cable Modem is Using Baseline Privacy

On a Cisco CMTS, one can use the **show cable modem** command to view the status of individual cable modems. There are several states that a modem utilizing Baseline privacy can appear in.

online

After a cable modem registers with a Cisco CMTS it enters the online state. A cable modem needs to get to this state before it can negotiate Baseline privacy parameters with a Cisco CMTS. At this point data traffic sent between the cable modem and CMTS is unencrypted. If a cable modem remains in this state and does not proceed to any of the states mentioned below, then the modem is not utilizing Baseline privacy.

online(pk)

The online(pk) state means that the Cable Modem has been able to negotiate an **Authorization Key**, otherwise known as a **Key Encryption Key (KEK)** with the Cisco CMTS. This means that the cable modem is authorized to use baseline privacy and has been successful in negotiating the first phase of baseline privacy. The KEK is a 56 bit key used to protect subsequent baseline privacy negotiations. When a modem is in online(pk) state data traffic sent between the cable modem and Cisco CMTS is still unencrypted as no key for the encryption of data traffic has been negotiated yet. Typically, online(pk) is followed by online(pt).

reject(pk)

This state indicates that the cable modem's attempts to negotiate a KEK have failed. The most common reason that a modem would be in this state would be that the Cisco CMTS has modem authentication turned on and the modem has failed authentication.

online(pt)

At this point the modem has successfully negotiated a Traffic Encryption Key (TEK) with the Cisco CMTS. The TEK is used to encrypt data traffic between the Cable Modem and Cisco CMTS. The TEK negotiation process is encrypted using the KEK. The TEK is a 56 or 40 bit key used to encrypt data traffic between the cable modem and Cisco CMTS. At this point baseline privacy is successfully established and running, therefore user data sent between the Cisco CMTS and cable modem is being encrypted.

reject(pt)

This state indicates that the cable modem was unable to successfully negotiate a TEK with the Cisco CMTS.

See below for a sample output of a show cable modem command showing cable modems in various states related to Baseline privacy.

Note: For more information on cable modem status, refer to Troubleshooting uBR Cable Modems Not Coming Online.

Timers Affecting the Establishment and Maintenance of Baseline Privacy

There are certain timeout values that can be modified to change the behavior of Baseline privacy. Some of these parameters may be configured on the Cisco CMTS and others through the

DOCSIS configuration file. There is little reason to change any of these parameters except for the KEK lifetime and the TEK lifetime. These timers may be modified to increase security on a cable plant or to reduce CPU and traffic overhead due to BPI management.

KEK Lifetime

The KEK lifetime is the amount of time that the Cable Modem and Cisco CMTS should consider the negotiated KEK to be valid. Before this amount of time has passed, the cable modem should renegotiate a new KEK with the Cisco CMTS.

You can configure this time using the Cisco CMTS cable interface command:

```
cable privacy kek life-time 300-6048000 seconds
```

The default setting is 604800 seconds which is equal to seven days.

Having a smaller KEK lifetime increases security because each KEK will last for a shorter period of time and hence if the KEK is hacked less future TEK negotiations would be susceptible to being hijacked. The drawback to this is that KEK re-negotiation increases CPU utilization on cable modems and increases BPI management traffic on a cable plant.

KEK Grace Time

The KEK grace time is the amount of time before the KEK lifetime expires, that a cable modem is meant to start negotiating with the Cisco CMTS for a new KEK. The idea behind having this timer is so that the cable modem has enough time to renew the KEK before it expires.

You can configure this time using the Cisco CMTS cable interface command:

```
cable privacy kek grace-time 60-1800 seconds
```

You can also configure this time using a DOCSIS configuration file by filling out the field labeled **Authorization Grace Timeout** under the Baseline Privacy tab. If this DOCSIS configuration file field is filled in then it takes precedence over any value configured on the Cisco CMTS. The default value for this timer is 600 seconds which is equal to 10 minutes.

TEK Lifetime

The TEK lifetime is the amount of time that the Cable Modem and Cisco CMTS should consider the negotiated TEK to be valid. Before this amount of time has passed, the cable modem should renegotiate a new TEK with the Cisco CMTS.

You can configure this time using the Cisco CMTS cable interface command:

```
     cable privacy tek life-time <180-604800 seconds>
```

The default setting is 43200 seconds which is equal to 12 hours.

Having a smaller TEK lifetime increases security because each TEK will last for a shorter period of time and hence if the TEK is hacked less data will be exposed to unauthorized decryption. The drawback to this is that TEK re-negotiation increases CPU utilization on cable modems and increases BPI management traffic on a cable plant.

TEK Grace Time

The TEK grace time is the amount of time before the TEK lifetime expires that a cable modem is meant to start negotiating with the Cisco CMTS for a new TEK. The idea behind having this timer is so that the cable modem has enough time to renew the TEK before it expires.

You can configure this time using the Cisco CMTS cable interface command:

```
     cable privacy tek grace-time 60-1800 seconds
```

You can also configure this time using a DOCSIS configuration file by filling out the field labeled **TEK Grace Timeout** under the Baseline Privacy tab. If this DOCSIS configuration file field is filled in then it takes precedence over any value configured on the Cisco CMTS.

The default value for this timer is 600 seconds which is equal to 10 minutes.

Authorize Wait Timeout

This time governs the amount of time a Cable Modem will wait for a response from a Cisco CMTS when negotiating a KEK for the first time.

You can configure this time in a DOCSIS configuration file by modifying the **Authorize Wait Timeout** field under the Baseline Privacy tab.

The default value for this field is 10 seconds and the valid range is 2 to 30 seconds.

Reauthorize Wait Timeout

This time governs the amount of time a Cable Modem will wait for a response from a Cisco CMTS when negotiating a new KEK because the KEK lifetime is about to expire.

You can configure this time in a DOCSIS configuration file by modifying the **Reauthorize Wait Timeout** field under the Baseline Privacy tab.

The default value for this timer is 10 seconds and the valid range is 2 to 30 seconds.

Authorization Grace Timeout

Specifies the grace period for reauthorization (in seconds). The default value is 600. The valid range is 1 to 1800 seconds.

Authorize Reject Wait Timeout

If a Cable Modem tries to negotiate a KEK with a Cisco CMTS, but is rejected, it must wait for the Authorize Reject Wait Timeout before re-attempting to negotiate a new KEK.

You can configure this parameter in a DOCSIS configuration file by using the **Authorize Reject Wait Timeout** field under the Baseline Privacy tab. The default value for this timer is 60 seconds and the valid range is 10 seconds to 600 seconds.

Operational Wait Timeout

This time governs the amount of time a Cable Modem will wait for a response from a Cisco CMTS when negotiating a TEK for the first time.

You can configure this time in a DOCSIS configuration file by modifying the **Operational Wait Timeout** field under the Baseline Privacy tab.

The default value for this field is 1 second and the valid range is 1 to 10 seconds.

Rekey Wait Timeout

This time governs the amount of time a Cable Modem will wait for a response from a Cisco CMTS when negotiating a new TEK because the TEK lifetime is about to expire.

You can configure this time in a DOCSIS configuration file by modifying the **Rekey Wait Timeout** field under the Baseline Privacy tab.

The default value for this timer is 1 second and the valid range is 1 to 10 seconds.

Cisco CMTS Baseline Privacy Configuration Commands

The following cable interface commands may be used to configure Baseline privacy and Baseline privacy related functions on a Cisco CMTS.

cable privacy

The cable privacy command enables the negotiation of Baseline privacy on a particular interface. If the **no cable privacy** command is configured on a cable interface, then no cable modems will be allowed to negotiate Baseline privacy when coming online on that interface. Use caution when disabling Baseline privacy because if a cable modem is commanded to use Baseline privacy by its DOCSIS configuration file, and the Cisco CMTS refuses to let it negotiate baseline privacy, then the modem may not be able to remain online.

cable privacy mandatory

If the **cable privacy mandatory** command is configured and a cable modem has baseline privacy enabled in its DOCSIS configuration file, then the cable modem must successfully negotiate and use Baseline privacy otherwise it will not be allowed to remain online.

If a cable modem's DOCSIS configuration file does not instruct the modem to use baseline privacy then the **cable privacy mandatory** command will not stop the modem from remaining online.

The **cable privacy mandatory** command is not enabled by default.

cable privacy authenticate-modem

It is possible to perform a form of authentication for modems that engage in Baseline privacy. When cable modems negotiate an KEK with the Cisco CMTS, modems transmit details of their 6 byte MAC address and their serial number to the Cisco CMTS. These parameters can be used as a username/password combination for the purpose of authenticating cable modems. The Cisco CMTS uses the Cisco IOS Authentication, Authorization and Accounting (AAA) service to do this. Cable modems that fail authentication are not allowed to go online. In addition, cable modems that do not use Baseline privacy are not affected by this command.

Caution: Since this feature makes use of the AAA service you need to make sure that you are careful when modifying AAA configuration, otherwise you may inadvertently lose the ability to log into and manage your Cisco CMTS.

Here are some sample configurations for ways to perform modem authentication. In these configuration examples, a number of modems have been entered into an authentication database. The 6 octet MAC address of the modem serves as a username and the variable length serial number serves as a password. Note that one modem has been configured with an obviously incorrect serial number.

The following partial sample Cisco CMTS configuration uses a local authentication database to authenticate a number of cable modems.

```
     cable privacy tek grace-time 60-1800 seconds
```

Another method of authenticating modems would be to employ an external RADIUS server. Here is a partial Cisco CMTS configuration example that uses an external RADIUS server to authenticate modems

```
     cable privacy tek grace-time 60-1800 seconds
```

Below is a sample RADIUS users database file with the equivalent information to the example above which used local authentication. The users file is utilized by a number of commercial and freeware RADIUS servers as a database where user authentication information is stored.

```
     cable privacy tek grace-time 60-1800 seconds
```

Shown below is the output of a **show cable modem** command executed on a Cisco CMTS which uses either of the above configuration samples. You will see that any Baseline privacy enabled modems not listed in the local authentication database, or with the incorrect serial number will enter the **reject(pk)** state and will not remain online.

The modem with SID 17 does not have an entry in the authentication database but is able to come online because its DOCSIS configuration file has not commanded it to use Baseline privacy.

The modems with SIDs 18, 21 and 22 are able to come online because they have correct entries in the authentication database

The modem with SID 19 is unable to come online because it has been commanded to use Baseline privacy but there is no entry in the authentication database for this modem. This modem would have recently been in the reject(pk) state to indicate that it failed authentication.

The modem with SID 20 is unable to come online because, although there is an entry in the authentication database with this modem's MAC address, the corresponding serial number is incorrect. At present this modem is in the reject(pk) state but will transition to the offline state after a short period.

When modems fail authentication a message along the following lines is added to the Cisco CMTS log.

```
%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted    BPI unauthorized Cable Modem
0001.9659.4461
```

The cable modem is then removed from the station maintenance list and will be marked as offline within 30 seconds. The cable modem will then most likely try to come on line once again only to be rejected again.

Note: Cisco does not recommend that customers use the **cable privacy authenticate-modem** command to stop unauthorized cable modems from coming online. A more efficient way of ensuring that unauthorized customers do not get access to a service provider's network is to configure the provisioning system such that unauthorized cable modems are instructed to download a DOCSIS configuration file with the network access field set to off. This way, the modem will not be wasting valuable upstream bandwidth by continually re-ranging. Instead, the modem will get to the **online(d)** state which indicates that users behind the modem will not be granted access to the service provider's network and the modem will only use upstream bandwidth for station maintenance.

Commands Used to Monitor the State of BPI

show interface cable X/0 privacy [kek | tek]—This command is used to display the timers associated with either the KEK or the TEK as set on a CMTS interface.

Below is an example output of this command.

```
CMTS# show interface cable 4/0 privacy kek
```

```
Configured KEK lifetime value = 604800

Configured KEK grace time value = 600



CMTS# show interface cable 4/0 privacy tek

Configured TEK lifetime value = 60480

Configured TEK grace time value = 600
```

show interface cable X/0 privacy statistic—This hidden command may be used to view statistics on the number of SIDs using baseline privacy on a particular cable interface.

Below is an example output of this command.

```
CMTS# show interface cable 4/0 privacy statistic



CM key Chain Count : 12

CM Unicast key Chain Count : 12

CM Mucast key Chain Count : 3
```

debug cable privacy—This command activates debugging of Baseline privacy. When this command is activated, whenever a change in Baseline privacy state or a Baseline privacy event occurs, details will be displayed on the console. This command only works when preceded with the **debug cable interface cable X/0** or **debug cable mac-address *mac-address*** command.

debug cable bpiatp—This command activates debugging of Baseline privacy. When this command is activated, whenever a Baseline privacy message is sent or received by the Cisco CMTS, the hexadecimal dump of the message will be displayed. This command only works when preceded with the **debug cable interface cable X/0** or **debug cable mac-address *mac-address*** command.

debug cable keyman—This command activated debugging of Baseline privacy key management. When this command is activated details of Baseline privacy key management are displayed.

Troubleshooting BPI

Cable Modems appear as online rather than online(pt).

If a modem appears in an online state rather than online(pt) then it generally means one of three things.

The first probable reason is that the cable modem has not been given a DOCSIS configuration file specifying that the cable modem utilize Baseline privacy. Check that the DOCSIS configuration file has BPI enabled in the Class of Service profile sent to the modem.

The second cause of seeing a modem in the online state could be that the modem is waiting before it commences negotiating BPI. Wait for a minute or two to see if the modem changes state to online(pt).

The final cause could be that the modem does not contain firmware that supports baseline privacy. Contact your modem vendor for a more recent version of firmware that does support BPI.

Cable Modems appear in reject(pk) state then go offline.

The most likely cause of a modem entering reject(pk) state is that cable modem authentication has been enabled with the **cable privacy authenticate-modem** command but AAA has been misconfigured. Check that the serial numbers and mac addresses of the affected modems have been correctly entered into the authentication database and that any external RADIUS server is reachable and functioning. You can use the router debugging commands **debug aaa authentication** and **debug radius** to get an idea of the status of the RADIUS server or why a modem is failing authentication.

Note: For general information on troubleshooting cable modem connectivity, refer to Troubleshooting uBR Cable Modems Not Coming Online.

Special Note - Hidden Commands

Any reference to hidden commands in this document is for informational purposes only. Hidden commands are not supported by the Cisco Technical Assistance Center (TAC). In addition hidden commands:

- May not always generate reliable or correct information
- May cause unexpected side effects if executed
- May not behave the same way in different versions of Cisco IOS Software
- May be removed from future releases of Cisco IOS Software at any time without notice

Related Information

- **CableLabs**
- **Authentication, Authorization, and Accounting (AAA)**
- **Technical Support - Cisco Systems**