CHAPTER 4

Configuring DOCSIS Baseline Privacy Interface on the Cisco uBR7200 Series

This chapter describes the DOCSIS 1.0 Baseline Privacy Interface (BPI), guidelines for configuring DOCSIS BPI on the Cisco uBR7200 series, and features of DOCSIS 1.1 Baseline Privacy Interface Plus (BPI+). This chapter contains the following sections:

Section	Description
"Baseline Privacy Interface Overview" section on page 4-1	Provides a description of DOCSIS 1.0 BPI, BPI key management, CM cummunication with the BPI, and illustrations.
"Enabling DOCSIS BPI" section on page 4-3	Provides guidelines for enabling DOCSIS 1.0 BPI on the Cisco uBR7200 series.
"DOCSIS 1.1 Baseline Privacy Interface Plus Overview" section on page 4-4	Provides an overview of the features in DOCSIS 1.1 BPI+.

Baseline Privacy Interface Overview

Baseline Privacy Interface (BPI) is defined as a set of extended services within the DOCSIS MAC sublayer. BPI gives subscribers data privacy across the RF network, encrypting traffic flows between the CMTS and CM.

Note Encryption/decryption is subject to export licensing controls.

The level of data privacy is roughly equivalent to that provided by dedicated line network access services such as analog modems or digital subscriber lines (DSL). BPI provides basic protection of service, ensuring that a CM, uniquely identified by its MAC address, can obtain keying material for services only it is authorized to access.

Note Because DOCSIS 1.0 BPI does not authenticate CMs, it does not protect against users employing cloned CMs masquerading as authorized CMs. Specific Cisco IOS releases provide protection against spoofing, and provide supporting commands that can be used to configure source IP filtering on RF subnets to prevent a user from using a source IP address that is not valid for the connected IP subnet.

BPI extends the definition of the MAC sublayer's SID. The *DOCSIS RF Interface Specification* (viewable at http://www.cablemodem.com/specifications/) defines a SID as a mapping between CMTS and CM to allocate upstream bandwidth and class of service management. When BPI is activated, the SID also identifies a particular security association and has upstream and downstream significance.

When BPI is operational, downstream multicast traffic flow that typically does not have a SID associated with it, now has a SID. The Privacy Extended Header Element includes the SID associated with the MAC Packet Data Physical Data Unit (PDU). The SID along with other components of the extended header element identifies to a CM the keying material required to decrypt the MAC PDU's packet data field.

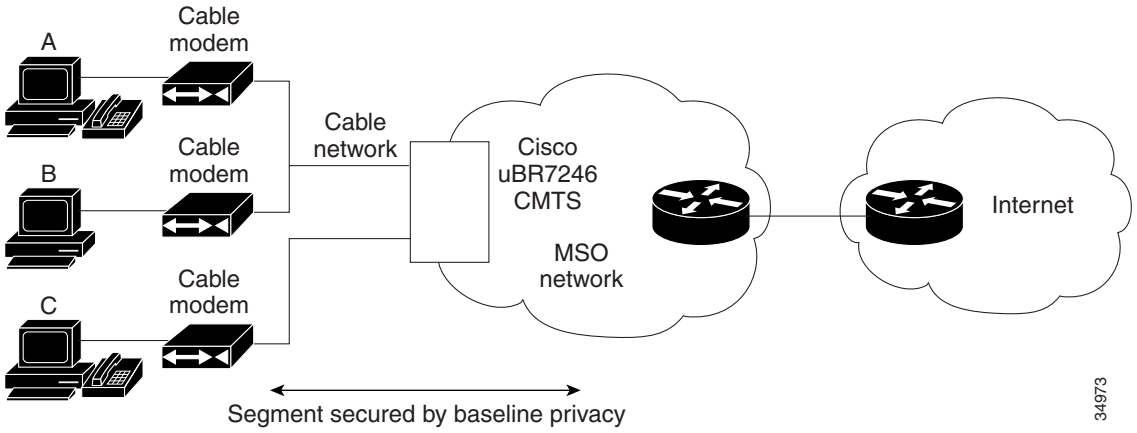
BPI's key management protocol runs between the CMTS and the CM. CMs use the protocol to obtain authorization and traffic keying material relevant to a particular SID from the CMTS and to support periodic reauthorization and key refresh.

The key management protocol uses RSA—a public key encryption algorithm—and the electronic codebook (ECB) mode of DES to secure key exchanges between the CMTS and a CM. Privacy is in the form of 56-bit (the default) or 40-bit encryption between the CMTS and CM. Since BPI is part of DOCSIS, all DOCSIS-certified CMs and qualified CMTS are fully interoperable. Figure 4-1shows a BPI architecture.

Note CMs must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment.

A SID's keying material has a limited life span. When the CMTS delivers SID keying material to a CM, it also provides the CM with the lifetime value.

Figure 4-1 BPI Network Example



BPI Key Management

BPI initialization begins with the CM sending the CMTS an authorization request, containing data identifying:

- CM—48-bit IEEE MAC address
- CM's RSA public key
- List of zero or more assigned unicast SIDs that have been configured to run BPI

At that time, BPI provides basic protection against theft of service by ensuring the CM, identified by its MAC address, can obtain keying materials only it is authorized to access. The CMTS replies with a list of SIDs on which to run BPI. The reply also includes an authorization key from which the CM and CMTS derive the keys needed to secure a CM's subsequent requests for additional encryption keys. After obtaining the traffic encryption key, the CMs begin to transmit encrypted data.

Differentiating Traffic Streams

BPI only encrypts data on the cable network and only encrypts the user data itself, not cable MAC headers. BPI also does not encrypt MAC management messages. After BPI is enabled, however, and encryption has been negotiated for a given SID, all user data sent via that SID is encrypted. BPI differentiates traffic based on SID alone.

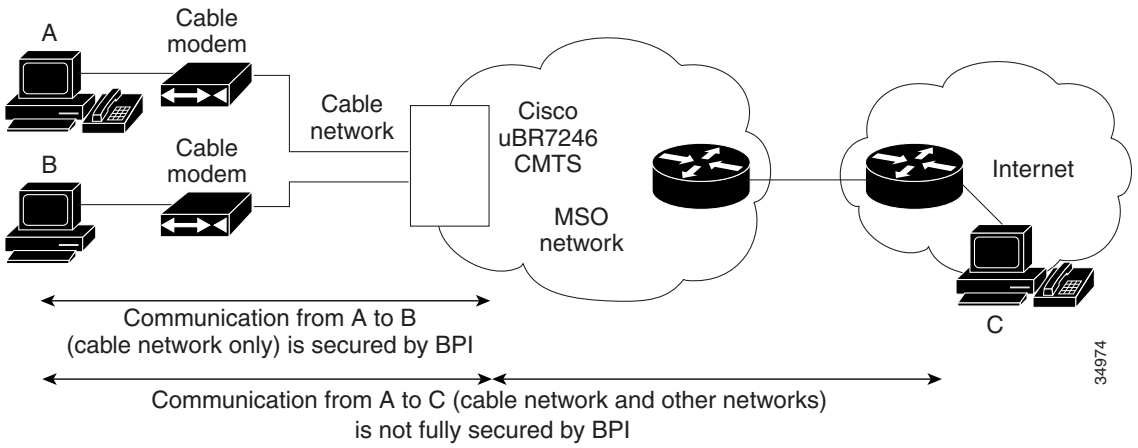
CM Communication with BPI

Figure 4-2 illustrates BPI communications. When user A sends packets to user B, the CM encrypts those packets using special keys specific to user's A CM. Packets are then transmitted to the CMTS where they are decrypted.

If user B is attached to the cable TV network, the CMTS then re-encrypts the information using a key specific to user B and the encrypted data is passed to user B's CM where it is decrypted and sent to user B. In this manner, an unauthorized user is not able to see unencrypted traffic between user A and user B.

Caution Since BPI occurs only on the cable TV network, however, all traffic going upstream will be decrypted as it passes the CMTS. If user A is attempting to communicate with someone beyond the cable network—user C—all traffic beyond the CMTS will not be encrypted.

Figure 4-2 BPI Encrypted Data on the Cable TV network



Enabling DOCSIS BPI

To enable BPI, choose software images at both the CMTS and CM that support the mode of operation. For the Cisco uBR7200 series software, choose an image with "k1" in its file name or BPI in the feature set description. For Cisco uBR924 cable access routers, all CM images from Cisco IOS Release 12.0(5)T1 or later support this by default. For earlier Cisco IOS release cable modem images, choose an image with "k1" in its file name or BPI in the feature set description.

Note For the CMTS, BPI is enabled by default when you select an image that supports BPI. For CMs, enable BPI via the DOCSIS configuration file using one of the provisioning tools identified in the "DOCSIS 1.0 Feature Support" section on page 1-49.

When baseline privacy is enabled, the Cisco uBR7200 series generates Traffic Encryption Keys (TEKs) for each applicable SID; 56-bit encryption/decryption is the default for Cisco uBR7200 series equipment.

The router uses the keys to encrypt downstream data and decrypt upstream traffic from two-way cable interfaces. The Cisco uBR7200 series router generates keys for unicast, broadcast, and multicast operation as appropriate. Keys are refreshed periodically and have a default lifetime of 12 hours.

DOCSIS 1.1 Baseline Privacy Interface Plus Overview

DOCSIS 1.0 included a BPI to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- Digital certificates provide secure user identification and authentication.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Multicast support.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Note BPI+ is described in the *Baseline Privacy Interface Plus Specification* (SP-BPI+-I07-010829), available from CableLabs (http://www.cablelabs.com).