Class of Service Restrictions and Outgoing Call Barring Features

Revised: July 2, 2009, OL-7680-24

The Cisco BTS 10200 Softswitch supports class of service restrictions and call barring options on outgoing calls. There are two suites of call restrictions—Class of Service (COS) restrictions and outgoing call barring (OCB). The COS and OCB features are assigned by the service provider. The COS feature cannot be controlled or deactivated by individual subscribers. The OCB feature can be activated, controlled, and deactivated by individual subscribers. These features are discussed in the following sections:

- "Class of Service Restrictions" section on page 3-2
- "Outgoing Call Barring (OCB)" section on page 3-14

Note For information on network features, see Chapter 1, "Network Features."

For information on subscriber features, see Chapter 2, "Subscriber Features."

Note Some features involve the use of other network elements (NEs) deployed in the service provider network, for example, gateways, media servers, announcement servers, eMTAs, and SIP phones. See the Component Interoperability section of the *Release Notes* for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 4.5.x software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list in the *Release Notes* certifies only that the required interoperation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Updates for Release 4.5.x

The following Release 4.5.x COS and OCB updates are included in this chapter:

- Updates were made to the section "Exemptions from COS and OCB Restrictions".
- The following changes were included in the section "Account Codes and Authorization Codes":
  - Tone-based options were enhanced.

- IVR-based options were added.

- The "Temporary Disconnect Treatment" section was added to explain the role of the COS feature in assigning a temporarily-disconnected status to subscribers.

- Additional capabilities and provisioning options were included in the "Outgoing Call Barring (OCB)" section These OCB enhancements were originally introduced in the *Release 4.4.1 OCB feature module*.

Class of Service Restrictions

The Cisco BTS 10200 Softswitch supports class of service (COS) restrictions on certain call types. The COS feature is assigned by the service provider and cannot be controlled or deactivated by individual subscribers.

This section covers the following topics:

- How to Use This Section of the Document

- COS Functional Description

- Exemptions from COS and OCB Restrictions

- National Call Restrictions (Toll Restrictions)

- Overview—Black and White List Features

- Casual Call (101XXXX) White and Black Lists (Number Blocking)

- National White and Black Lists (Number Blocking)

- International White and Black Lists (Number Blocking)

- Originating Line Information White and Black Lists

- Nature of Dial White and Black Lists

- Blocking Flags

- Account Codes and Authorization Codes

- ANI Screening on Incoming Calls

- Temporary Disconnect Treatment

- COS Restriction Priorities

- High-Level Flowchart of COS Screening Process

How to Use This Section of the Document

This section describes the COS feature and the impact of certain provisionable parameters. It should be used in conjunction with the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip For the sequence of commands used to provision this feature, see the *COS provisioning procedure* in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

COS Functional Description

COS restrictions prevent certain types of calls from being completed from a particular line or station. The service provider can:

- Provision COS restrictions for individual subscribers, groups of subscribers, trunk groups (TGs), automatic number identification (ANI), and authorization codes.

- Prohibit calls based on dialing plans and call types. (Call types for COS screening are contained in the Nature of Dial (NOD) table.)

When a call is blocked, the calling party receives a blocking treatment such as reorder tone or announcement.

Exemptions from COS and OCB Restrictions

Certain types of calls are exempt from both COS and OCB restrictions:

- Emergency calls (calls with call-type=EMG)—These calls are never subject to COS and OCB screening. The system always exempts emergency calls from COS and OCB screening without considering any provisioned parameters. Note that it is possible to provision AMBULANCE, FIRE, and POLICE as subtypes of EMG in the Destination table. If provisioned as subtypes of EMG, these types are given the same treatment as EMG.

- Call types on either of the NOD exception lists—The service provider can provision exception lists to override COS and OCB screening on certain types of calls. The types of calls on these lists can include, for example, repair calls, toll-free calls, and so forth. The applicable types of calls are listed in the NOD table. These exceptions are applicable at the switch level (all office codes) and cannot be specified for individual subscribers. There are two NOD exception lists:

    - Trigger NOD Escape List table—If the service provider provisions a NOD type/trigger ID pair in the Trigger NOD Escape List (trigger-nod-escape-list) table, that NOD type will not trigger COS or OCB screening.

    - NOD Restrict List—If the service provider provisions a NOD type in the NOD Restrict List (nod-restrict-list) table, that NOD type can trigger COS or OCB screening, but will be exempted at the first screening step.

Tip   Cisco recommends that you use trigger-nod-escape-list to provide this function, because it uses system resources more economically. It is not necessary to provision both lists for this function.

Note   See the *complete list of NOD values* in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

National Call Restrictions (Toll Restrictions)

The national call restrictions are used to allow or restrict calls to destinations based on a predefined grouping of local lines, LATA, state, country, or group of countries. Customers can subscribe to one of the following:

- All North American Numbering Plan (NANP) calls—All calls within NANP are allowed (can be applied only to calls originated in NANP).

- National only—Only calls terminating within the country are allowed.
- Intrastate only—Only calls within the state are allowed.
- IntraLATA only—Only calls within the LATA are allowed, including intraLATA toll calls (can be applied only to calls originated in NANP).
- Local only—Only local calls are allowed.

For NANP operator calls (0+NPA-NXX-XXXX), NANP call restriction screening is not performed, even if the NANP call restriction is provisioned in the cos-restrict table for the calling party.

Overview—Black and White List Features

The service provider can provision a list of directory numbers (DNs) to appear on a black list or a white list as follows:

- Black-listed calls do not undergo further screening, and all calls on this list are rejected. This is called number blocking.
- White-listed calls are subject to additional normal OCB restrictions based on call type (if the OCB feature is assigned to the subscriber and activated).

The service provider can also create white and black lists based on originating line information (OLI) and nature of dial (NOD).

Note   OCB is a subscriber feature that the service provider can assign to any subscriber line. After OCB is assigned, it is controlled by the individual subscriber. (Typically, OCB is used by service providers outside the North American market.)

For the black/white-list functionality of the OCB feature, the service provider should provision the desired black/white-list COS restrictions for each OCB subscriber, and assign a COS-RESTRICT-ID for the subscriber. This ensures that the black and white list restrictions are in effect, even if the user deactivates OCB. For a complete description of the OCB feature, see the "Outgoing Call Barring (OCB)" section on page 3-14.

The service provider can provision an exception list to override COS and OCB screening on certain types of calls. See the "Exemptions from COS and OCB Restrictions" section on page 3-3.

For details on each type of black/white list, see the following sections:

- Casual Call (101XXXX) White and Black Lists (Number Blocking)
- National White and Black Lists (Number Blocking)
- International White and Black Lists (Number Blocking)
- Originating Line Information White and Black Lists
- Nature of Dial White and Black Lists
- Blocking Flags

Casual Call (101XXXX) White and Black Lists (Number Blocking)

The casual call white and black lists are used to allow or restrict calls dialed with a casual code prefix (101XXXX). The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be provisioned:

- No casual calls allowed—User cannot make 101XXXX calls.
- All casual calls allowed—User can make 101XXXX calls.
- 101XXXX white list—Only a predefined set of XXXX codes can be dialed.
- 101XXXX black list—All XXXX codes can be dialed except for a predefined set.

For NANP operator calls (0+NPA-NXX-XXXX) and international operator calls (01+CC+NN), casual-call screening is not performed, even if the casual-call restriction is provisioned in the cos-restrict table for the calling party.

National White and Black Lists (Number Blocking)

The national white and black lists are used to allow or block national calls based on a predefined list of DNs. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No restrictions.
- National white list—Only calls on a predefined prefix list can be called. The list could consist of full or partial DNs (for example, NDC or NDC-EC codes, or NPA or NPA-NXX codes for North America).
- National black list—All calls on a predefined prefix list are blocked. The list could consist of full or partial DNs (for example, NDC or NDC-EC codes, or NPA or NPA-NXX codes for North America).

For NANP operator calls (0+NPA-NXX-XXXX), NANP call restriction screening is not performed, even if the NANP call restriction is provisioned in the cos-restrict table for the calling party.

The national white black list table checks telephone numbers only for the following call types: local, intralatatoll, interlatatoll, national (ITU only), toll, intl-wz1, international, casual, 900, premium, 976, da, da-toll, 0-plus, 0-minus, 01-plus, tw, info and non-emergency. The system does not check this list if the NOD is not one of these call types. For example, if an 800 number is added to this table, the number is not checked, since an 800 number is call type toll-free, and toll-free is not a supported call type.

International calls within NANP are screened against the national white and black lists, and not against the international white and black lists.

International White and Black Lists (Number Blocking)

The international white and black lists are used to allow or block calls made outside the country. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No international calls allowed—Does not allow any international calls.
- International white list—Allows only those calls that have a country code (CC) noted in the white list.
- International black list—Does not allow any calls that have a CC noted in the black list.

- All international calls allowed—No restrictions are applied on international calls.

For international operator calls (01+CC+NN), international call restriction screening is not performed, even if the international call restriction is provisioned in the cos-restrict table for the calling party.

International calls within NANP will be screened against the national white and black lists, and not against the international white and black lists.

Originating Line Information White and Black Lists

The originating line information (OLI) white and black lists (also referred to as II white and black lists) are used to allow or block calls made from certain types of lines, such as hotels, prisons, and so forth. This is a Tandem call screening function. The applicable COS can be set up to perform either white list screening or black list screening, but not both. The following restrictions can be applied:

- No OLI screening performed.
- Use the II white/black screening list as a white list—Allows the specified OLI types to place calls.
- Use the II white/black screening list as a black list—Blocks calls from the specified OLI types.

✎ **Note**   II digits 24 and 25 are exempt from COS screening (these are translated toll-free 8XX calls from POTS lines).

Nature of Dial White and Black Lists

The nature of dial (NOD) white and black lists (NOD-WB-LIST) are used to allow or block certain categories of calls, such as casual dialing (dialing around), time/weather, international operator assistance, premium calls, toll calls, toll-free calls, and so forth. The following restrictions can be applied:

- No NOD screening performed.
- Use the NOD white/black screening list as white list—Allow the specified NOD types to be called.
- Use the NOD white/black screening list as black list—Block calls to the specified NOD types.

✎ **Note**   To block international calls that originate within the 48 contiguous U.S. states and terminate in World Zone 1 (outside of the contiguous 48 states but within NANP), set the NOD token to INTL-WZ1 in the NOD White Black List table.

✎ **Note**   Certain types of calls that are exempt from both COS and OCB restrictions. See this information in the "COS Functional Description" section on page 3-3.

✎ **Note**   Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for a complete list of NOD types.

Blocking Flags

The service provider can provision the blocking flags listed below. These have the same effect as provisioning the NOD black list for the same feature.

Tip All call types that can be blocked using blocking flags can *also* be blocked by placing that call type on the NOD black list. Cisco recommends using the NOD black list.

- Block 900 (premium) calls—Blocks all calls of the form 1-900-XXX-XXXX.
- Block 976 (local information) calls—Blocks all calls of the form 976-XXXX or NPA-976-XXXX.
- Block info calls—Blocks all calls to information services.
- Block time/weather calls—Blocks all calls to time and weather services.
- Block directory assistance (DA) calls—Blocks all directory assistance calls of the form 411, 1+411 or NPA-555-XXXX.
- Block NANP operator assistance calls—Blocks all calls to an operator within NANP, specifically, 0 calls and 0+ calls (0+NPA-NXX-XXXX).
- Block international calls—The behavior of this flag depends upon the location of the originating station:
  - For call that originate from locations outside NANP, this flag blocks all calls terminating outside the country.
  - For calls that originate from locations inside NANP, this flag blocks all calls terminating outside NANP.

    Note For calls that originate from locations inside NANP, to block calls terminating outside the country but inside NANP (for example, calls from the United States to Canada), use the INTL-WZ1 token in the NOD White Black List.

- Block international operator assistance calls—Blocks all calls to an operator outside the country, including 01+ calls (01+CC+NN).

Account Codes and Authorization Codes

The Cisco BTS 10200 Softswitch supports account code and authorization code features as described in this section. These features are part of the COS features, and include the collection and screening of digits on calls. The individual or business can use this feature to help restrict or block certain types of outgoing calls.

Tone-Based and IVR-Based Options

The service provider can provision the system to use either a tone-based procedure or an IVR-based procedure for collecting and screening the digits.

Note Cisco recommends that you use IVR-based COS only in cases where the originating MGW or TGW is unable to play tones to the caller. The IVR-based COS feature for ISDN trunk is for the North American market only. It is not supported for SS7, H.323, or SIP endpoints.

- The tone-based procedure requires that the originating MGW be capable of playing tones to the caller. When an account or authorization code is required during COS screening, the Cisco BTS 10200 Softswitch instructs the MGW to play the appropriate tones and collect digits. After the digits are collected, the call proceeds or is blocked based on COS restrictions.

- The IVR-based procedure is used when the originating MGW is not capable of playing tones to the caller. This is typically true of TGWs and devices such as PBXs connected over ISDN PRI trunks at the customer premises. When an account or authorization code is required during COS screening, an IVR server plays the appropriate prompts and collects digits entered by the handset user. After the digits are collected, the call proceeds or is blocked based on COS restrictions.

Tone-Based Operation

This section describes the tone-based operation of account codes and authorization codes. It also describes provisionable prompt-delay timers that can be used for certain scenarios involving PBX systems.

Account Codes (Nonverified) Tone-Based Operation

Account codes provide collection of 2 to 12 digits to allow call charging to user projects, departments or special accounts. The user activates account codes by dialing a number (usually a long-distance call) that requires an account code for call completion. A prompt tone is issued after the digits are dialed. The user then enters an account code of a specified length. These account codes are not verified. (See the next section for verified account codes.) The account code is provided in the call detail records (CDRs) associated with the call. Account codes are not collected for any of the following call types:

- National operator calls
- International operator calls
- Local calls

Authorization Codes (Verified Account Codes)—Tone-Based Operation

Authorization codes, also referred to as verified account codes, can be used by an intended user or group to override certain COS calling restrictions. For example, long-distance calls could be restricted on certain phones, such as phones in a lobby or conference room, unless the user knows a valid authorization code. When an authorization code is required, the user is prompted via a tone. The user can override the restriction by dialing an authorization code that has enough privileges to make long-distance calls. Authorization codes can be from 3 to 23 digits in length.

The user takes the following action when an authorization code is required:

- The user goes off hook and receives a dial tone.
- The user dials a DN. The system determines that an authorization code is required and returns a confirmation tone (2 beeps) to the user.
- The user enters the digits for the authorization code.
    - If the user enters the correct authorization code, the call is screened based on COS assigned to that authorization code. If this authorization code has appropriate privileges, the call is allowed.

– If the user enters a code that is incorrect, does not have appropriate privileges for the call being attempted, or if the associated account is invalid, the call is diverted to a preselected announcement.

Note Authorization codes can be used to override call category restrictions, but cannot be used to override black/white lists. For example, an authorization code can be used to override "no international calls allowed", but cannot be used to override any type of black/white list.

Use of Prompt-Delay Timers for PBX System Connected via IAD

When an account code or authorization code is required, a caller connected to an IAD or MGW is provided with a prompting tone. However, if a caller is connected to a PBX that is connected to an IAD (via CAS protocol), the PBX might not be capable of cutting through the prompting audio quickly enough for the caller to actually receive the prompt. To help resolve this problem, the Cisco BTS 10200 Softswitch has provisionable tokens that can be used to introduce delay before playing the account-code or authorization-code prompt. When this prompt delay is provisioned appropriately, PBX users are able to hear the confirmation tone when they make calls requiring an access code. The option to delay the MGCP RQNT message applies only to CAS trunk groups without main-subscriber, or CAS trunk groups with main-subscriber whose category is PBX. The delay is provisionable via CLI using the following tokens in the CA-CONFIG table:

- ACCT-CODE-PROMPT-DELAY, for introducing delay prior to playing the account code prompt.
- AUTH-CODE-PROMPT-DELAY, for introducing delay prior to playing the authorization code prompt.

Note The prompt-delay feature is not supported for SS7, H.323, ISDN, or SIP endpoints, or for analog subscriber lines.

For detailed descriptions of these tokens, see the *Cisco BTS 10200 Softswitch Command Line Reference Guide*. For a list of commands used to provision these features, see the *Cisco BTS 10200 Softswitch Provisioning Guide*.

IVR-Based Operation

The system supports IVR-based operation of account codes and authorization codes for ISDN trunks. The feature interfaces with, and is dependent on, the services of a network IVR server. When an account or authorization code is required during COS screening, an IVR voice path is established between the IVR server and the ISDN trunk on the TGW/MGW/IAD at the customer site.

Prerequisites for IVR-Based Operation

For IVR-based capabilities, the Cisco BTS 10200 Softswitch interfaces with, and is dependent on, the services of an IVR server. The feature also requires all the network setup for a basic feature call. This feature further requires the PacketCable Basic Audio Package (BAU) interface for managing and controlling IVR endpoints. See PacketCable document PKT-SP-ASP-102-010620.

Restrictions and Limitations for IVR-Based Operation

The following restrictions and limitations apply to the implementation of the IVR-based COS account and authorization codes:

- The IVR-based account and authorization code capability is supported only for ISDN PRI trunks and only in the North American market.

- The system does not support the IVR-based account and authorization code capability for SS7, H.323, and SIP endpoints.

- The system does not support local IVR capability. (Local-IVR involves using IVR resources of the ingress gateway.)

- In the Cisco BTS 10200 Softswitch, authorization and account codes reported using IVR are not appended to the *DialedDigit* parameter issued to billing record because the IVR digits are not processed in the Call Agent.

Feature Provisioning

The following tokens in the Class of Service Restrict (cos-restrict) table affect the behavior of this feature:

- To control the type of prompt played to the user, set the PROMPT-METHOD token to TONE (default) or IVR.

- To specify whether to permit calls when an IVR server fails, set the ALLOW-CALLS-ON-IVR-FAILURE token to Y (default) or N.

For general COS provisioning, see the *Class of Service (COS) provisioning procedure* in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

To provision IVR support for features that use the IVR functionality, see the applicable feature provisioning procedure in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

ANI Screening on Incoming Calls

Automatic number identification (ANI) screening is a service commonly found in Tandem switches, and is used for long-distance access service. The ANI is the number of the calling party (NDC + EC + DN). Full or partial ANIs can be specified for screening. The ANI screening feature validates the ANI on incoming trunk group (TG) calls from the public switched telephone network (PSTN) before routing. All ANIs to be screened are stored in the Feature Server database. If an ANI is not available, or does not appear in the Feature Server ANI table, the call is considered as a casual call. The TG restrictions are checked to see if casual calls are allowed. If casual calls are not allowed, the call is denied and routed to an announcement. If the ANI exists in the table, the ANI status is checked next. The ANI status can either be allowed or blocked. If the status is blocked, the call is blocked and routed to an announcement. COS can also be applied on an ANI basis.

Temporary Disconnect Treatment

The service provider can designate a subscriber as temporarily disconnected (for example, for nonpayment of bills) and use COS screening to limit the types of calls the subscriber is allowed to make. For example, a special set of COS restrictions can allow temporarily-disconnected subscribers to call only the repair number.

For subscribers with STATUS=TEMP-DISCONNECTED in the Subscriber table, the system ignores the COS restriction ID for the subscriber (in the Subscriber Profile table), and instead uses the TEMP-DISC-COS-RESTRICT-ID token in the Point of Presence (POP) table.

> **Note** For a full description, see the "Temporarily Disconnected Subscriber Status and Soft Dial Tone" section in Chapter 2, "Subscriber Features."

COS Restriction Priorities

For any call, it is possible that a combination of call categories are applicable. Under these conditions, the system performs Black White List screening first. If the call passes (is allowed from) Black White List screening, then the system applies COS restriction screening.

COS restrictions can be assigned to any ANI, authorization code, trunk group, or POTS subscriber. When multiple COS restrictions apply to a trunk call, the system uses the order of precedence as follows:

1. Use the COS assigned to ANI if found in the ANI screening table.

2. If not found in ANI screening table, use the COS assigned to the TG.

3. If an authorization code is required, then use the COS assigned to authorization code.

When a call is blocked due to COS screening, the call event shows which type of screening blocked the call. The service provider can provision the treatment of blocked calls, and can include, for example, playing an announcement or sending a cause code to the originator.

High-Level Flowchart of COS Screening Process

Figure 3-1 and Figure 3-2 show a high-level flowchart of the COS screening process. The flowchart is split into two parts (two drawings) for easier viewing.

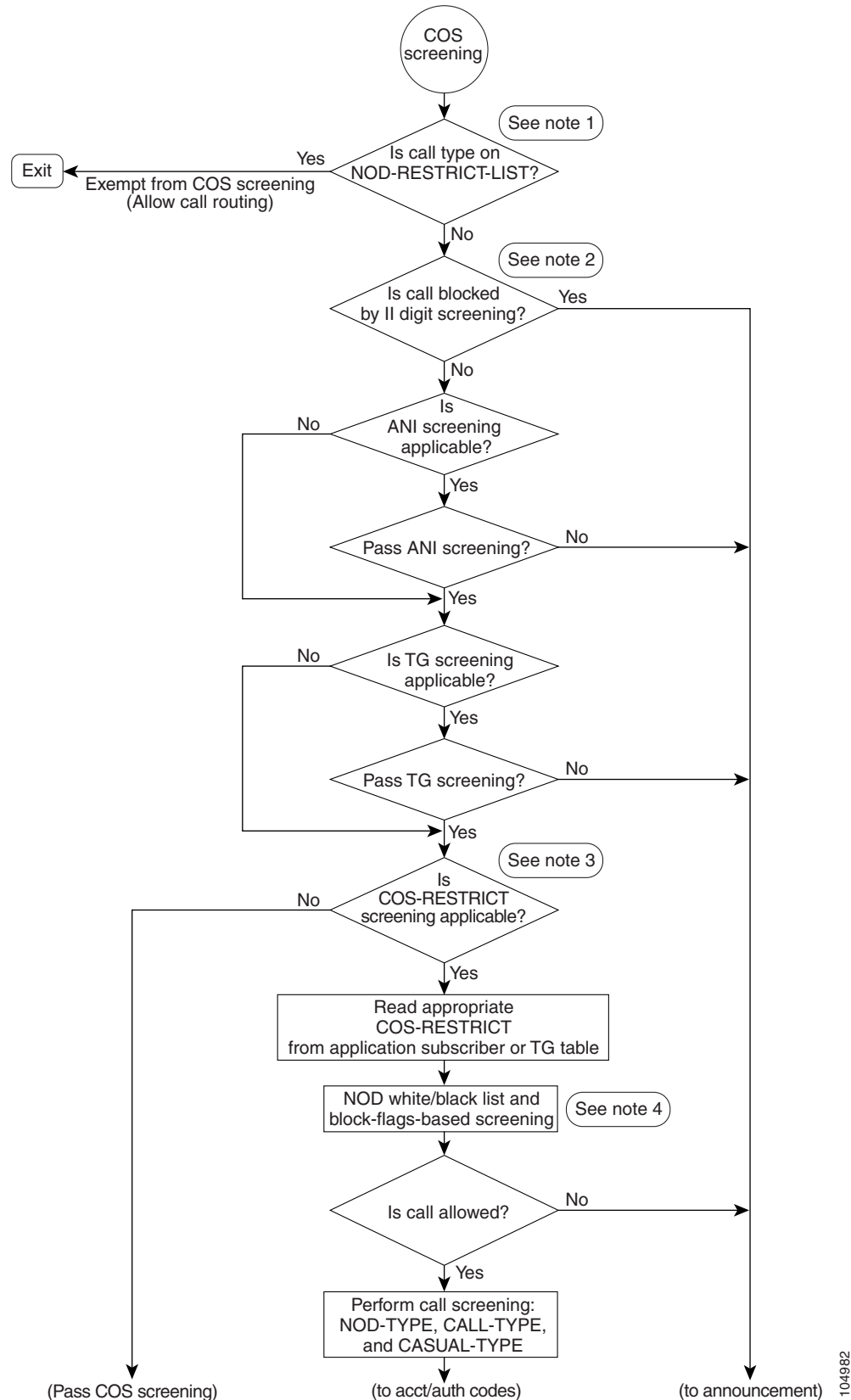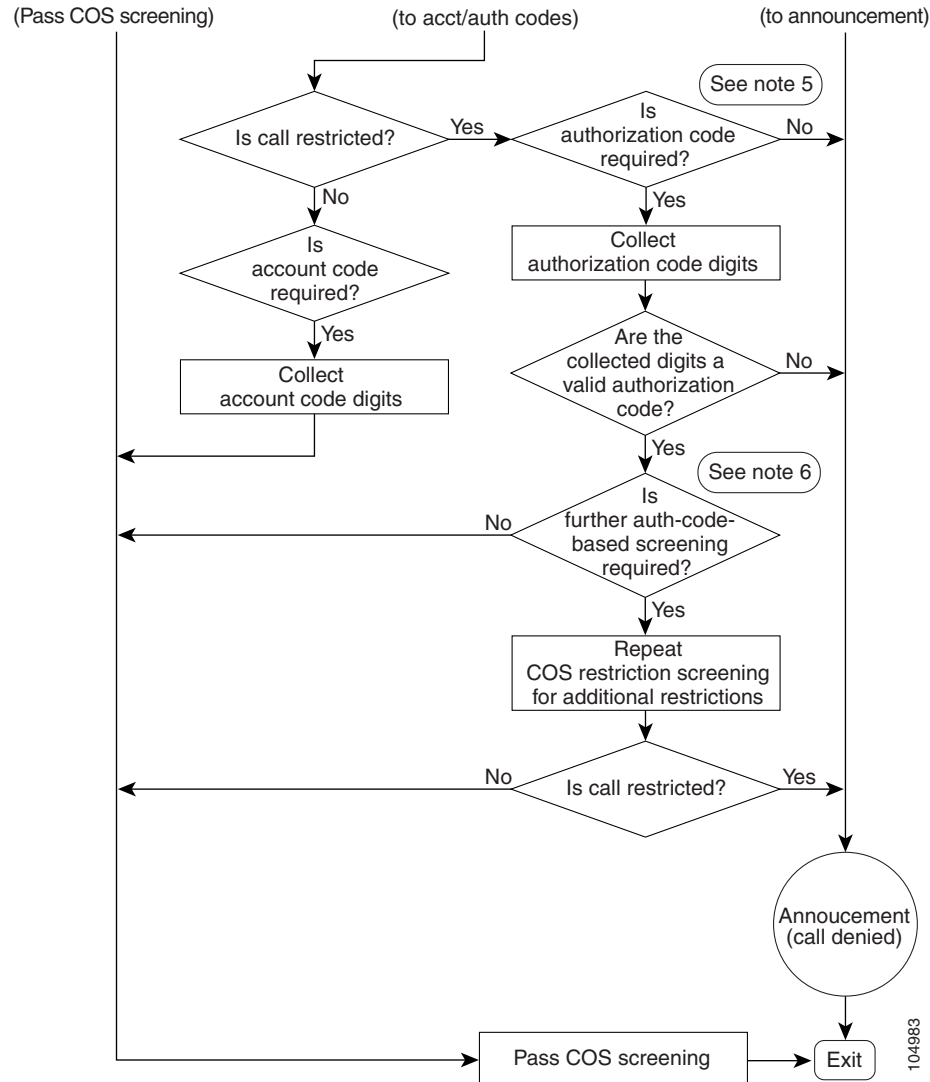***Figure 3-1***   ***COS Screening Process (Part 1)***

Figure 3-2   COS Screening Process (Part 2)

Notes for Figure 3-1 and Figure 3-2:

1. Call types on the NOD-RESTRICT-LIST are exempt from COS screening.

2. II = 24 and 25 are reserved for translated toll-free calls and are exempt from II screening.

3. COS-RESTRICT screening is applicable if either the subscriber or the TG has an associated COS-RESTRICT-ID.

4. Block flags are as follows:

   – BLOCK-900

   – BLOCK-976

   – BLOCK-DA

   – BLOCK-INFO

   – BLOCK-TW

    – BLOCK-INTL

    – BLOCK-NANP-OPER-ASSIST

    – BLOCK-INTL-OPER-ASSIST

✎ **Note** NOD-WB-LIST has a higher precedence that the block flags during screening.

5. The initial check of the authorization code is based on the provisioned value for AUTH-CODE-ALLOW in the applicable COS-RESTRICT table.

6. The additional check of authorization code is based on the COS-RESTRICT-ID provisioned in the applicable AUTH-CODE table.

Outgoing Call Barring (OCB)

This section describes the Cisco BTS 10200 Softswitch support for the outgoing call barring (OCB) feature. This feature was introduced in Release 3.2, and enhanced in Release 4.4.1. The OCB feature allows an individual subscriber or business group administrator to restrict certain types of outgoing calls. Once OCB is provisioned and activated on a calling line, the OCB restrictions are transparently invoked on all outgoing calls.

The Cisco BTS 10200 Softswitch support for the OCB feature complies with the International Telecommunications Union standard *ITU-T I.255.5, Outgoing Call Barring*.

✎ **Note** The class of service (COS) feature is an optional functionality (subset) of OCB. The service provider can provision the COS feature by itself, without the OCB feature. The details are discussed later in this section.

✎ **Note** Certain types of calls that are exempt from both COS and OCB restrictions. See this information in the "COS Functional Description" section on page 3-3.

This section covers the following topics:

- OCB Highlights (Release 3.2)
- OCB Highlights (Release 4.4.1)
- How To Use This Section of the Document
- OCB for Release 3.2
- OCB Enhancements for Release 4.4.1

OCB Highlights (Release 3.2)

The following list highlights some of the major functions and behaviors for the OCB feature in Release 3.2:

- K-values (call-barring levels) are K=1 (all calls), K=2 (domestic long distance and international), and K=3 (international). These values are automatically enabled for the handset user when the OCB feature is provisioned by the service provider.

- The private identification number (PIN) and PIN length are provisioned by the service provider. They cannot be provisioned by the user via the handset, and cannot be changed by the user.

- If a user forgets the original password, the service provider can, with proper authorization, reset the password. The service provider (after proper authorization) can provision a new password and inform the subscriber.

- Only one K-value can be active at any time on a specific subscriber line.

- If the user deactivates OCB via the handset, the system deactivates OCB without checking the K-value the user enters.

- If the user attempts to reactivate OCB to the same K-value that is currently active, the system treats the attempt as a new attempt, and provides the same success announcement as for the previous activation. If the user attempts to activate OCB to a different K-value than is currently-activated, the system plays the appropriate announcement.

OCB Highlights (Release 4.4.1)

Release 4.4.1 introduced extensions to the OCB feature. It is important to understand that the Release 4.4.1 extensions to OCB are additions to the initial Release 3.2 OCB feature. If you provision a Release 4.4.1 system using Release 3.2 OCB provisioning steps, the OCB feature will, by default, operate exactly as it did when initially introduced in Release 3.2.

The following list describes the OCB enhancements introduced with Release 4.4.1:

- The range of K-values (call-barring levels) is 1 through 9, and the service provider can provision each of the 9 values for specific call types.

- K-values can be mapped to call-types at the POP or at the office level. If K-values are not mapped at the POP level, the software checks to see if they are mapped at the office level. If K-values are not provisioned at either the POP or office level, OCB defaults to the hard-coded mapping of the three K-values as in Release 3.2. K-value mapping need not be configured per subscriber.

- Only one K-value can be active on a specific subscriber line.

- The service provider can provision three deactivation options for the handset user, including the option to deactivate only if the user enters a currently-active K-value.

- The PIN length is provisioned by the service provider and cannot be provisioned by the user via the handset, and cannot be changed by the user. The initial PIN setup can be performed either by the service provider, or can be provisioned for the user to set up using the handset. However, the initial PIN cannot be changed by the handset user.

- If a user forgets the original password, the service provider (after proper authorization) can reset the password.

How To Use This Section of the Document

If you provision a Release 4.4.1 system using Release 3.2 OCB provisioning steps, the OCB feature will, by default, operate exactly as it did when initially introduced in Release 3.2.

This section describes the OCB feature and the impact of certain provisionable parameters. It should be used in conjunction with the *Cisco BTS 10200 Softswitch Provisioning Guide.*

Tip   For the sequence of commands used to provision this feature, see the *OCB provisioning procedure* in the *Cisco BTS 10200 Softswitch Provisioning Guide.*

For a list of cause codes and announcements, see the *Cisco BTS 10200 Softswitch Provisioning Guide*.

For a list of traffic measurements (counters), see the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

For billing procedures and data, see the *Cisco BTS 10200 Softswitch Billing Guide*.

OCB for Release 3.2

The outgoing call barring feature allows an individual subscriber or business group administrator to restrict certain types of outgoing calls. Once the OCB feature is provisioned and activated on a calling line, the OCB restrictions are transparently invoked on all outgoing calls.

OCB Subscription and Provisioning (Release 3.2)

The service provider sets up OCB service at the request of the subscriber. There are a number of service provider provisionable parameters that affect the behavior of the feature on the subscriber line:

- Vertical service code (VSC)—ASCII strings that the user must enter to access OCB activation, deactivation, and interrogation options. The recommended values are *54*, #54* and *#54# as used in the examples below. However, VSCs are not preprovisioned in the system. The service provider can provision these values with any valid unique ASCII string up to five characters long.

    Note   The valid formats for VSC ASCII strings are listed in the VSC table specification in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. The preprovisioned VSC values are listed in the Vertical Service Code appendix of the same document.

- Private identification number (PIN)—A digit string that the user must enter for authorization to set OCB activation and deactivation options from his or her local phone.

- PIN length (PIN-LEN)—The number of digits required for a valid PIN.

    Note   The PIN and PIN-LEN are provisioned by the service provider. They cannot be provisioned by the user via the handset, and cannot be changed by the user.

- Allowed activation/deactivation attempts and lockout parameters—Parameters can be provisioned to limit the number of times that a user can enter incorrect data or PIN within a specified time. If the limit is exceeded, the system ignores further activation and deactivation attempts for a provisionable length of time (lockout period).

OCB Activation and User Options (Release 3.2)

OCB activation (OCBA) allows a user to activate OCB and select various call barring options on his or her local phone. The user does this by dialing *54*K-VALUE<PIN># (the trailing # is optional to signify the end of entry). The parameters are defined as follows:

- *54* is the VSC the user must enter on his or her handset to access the OCBA feature

- K-VALUE is the parameter that determines the type of outgoing calls to be barred:

    - K-VALUE=1: all outgoing calls barred

    - K-VALUE=2: domestic long distance and international outgoing calls barred

    - K-VALUE=3: international outgoing calls barred

> **Note** Emergency calls (calls with call type set to EMG) are not barred, regardless of the specified K-value.

- <PIN> is the assigned private digit string that the user must enter. A success announcement is given on a successful activation, and an error announcement, indicating the type of error, is given if activation is unsuccessful.

> **Note** The K-VALUE can be changed only when the OCB feature is in the deactivated state.

If a user enters incorrect data or PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning (Release 3.2)" section on page 3-16.

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters a value for K-VALUE that is not 1,2, or 3.

- The user tries to activate OCB on a fresh system (a system with no initial PIN entry in the SUBSCRIBER-FEATURE-DATA table). In this case, the user receives the error announcement.

OCB Deactivation (Release 3.2)

OCB deactivation (OCBD) allows a user to deactivate all OCB on his or her local phone. The user does this by dialing #54*K-VALUE<PIN>#. The parameters are defined as follows:

- #54* is the VSC the user must enter on his or her handset to access the OCBD feature

- K-VALUE must be entered as 1, 2, or 3. However, the actual value is ignored by the system, because OCBD deactivates all call barring.

- <PIN> is the same as for OCBA.

A success announcement is given on a successful deactivation, and an error announcement, indicating the type of error, is given if deactivation is unsuccessful.

> **Note** See the *Cisco BTS 10200 Softswitch CLI Reference Guide* for provisioning details.

If a user enters incorrect data or PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning (Release 3.2)" section on page 3-16.

OCB Interrogation (Release 3.2)

OCB interrogation allows a user to check the level of outgoing call restrictions on his or her local phone. The dial string for OCB Interrogation is *#54#. No PIN is required to use this feature. The system provides an appropriate announcement to the user.

OCB Invocation and Screening (Release 3.2)

For a calling party that is subscribed to OCB, and has activated the feature, the feature is invoked for every call made after the called party digits are dialed. There is no user driven invocation method involved for the feature. Once provisioned for a calling party, and activated on the calling party's line, the invocation is handled automatically by the Cisco BTS 10200 Softswitch.

OCB Lockout Behavior

The LOCK-OUT, TO (timeout), and FAIL-CNT (fail count) tokens in the feature table are intended to prevent unauthorized changes or bypassing of OCB screening. If a user repeatedly enters the password or other OCBA/OCBD data incorrectly on the handset, the system can lock the line against both OCBA and OCBD. These tokens control the lockout behavior as described in Table 3-1.

Tip Note that there is no service lockout when either the TO or FAIL-CNT token is set to zero.

Table 3-1   OCB Lockout Behavior

OCB Tokens in Feature Table			Lockout Behavior Due to OCBA/OCBD Misuse
LOCK-OUT	TO	FAIL-CNT	
n/a	n/a	0	No service lockout
n/a	0	n/a	No service lockout
0	1 or greater	1 or greater	OCBA and OCBD are locked out indefinitely after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes
1 or greater	1 or greater	1 or greater	OCBA and OCBD are locked out for <LOCK-OUT> minutes after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes

How to Coordinate OCB and COS Provisioning

Typically, service providers in North America provide the COS feature set, but not the OCB feature set, to their customers. In the rest of the world, service providers typically provide OCB. On the Cisco BTS 10200 Softswitch, the black/white list functionality of OCB is contained in the COS module. Therefore, to provide black/white-list functionality with OCB, you must:

- Assign the OCB feature and provision the desired OCB options for each subscriber.
- Provision the desired black/white-list COS restrictions for each OCB subscriber, and assign a COS-RESTRICT-ID for the subscriber. This ensures that the black and white list restrictions are in effect, even if the user deactivates OCB. It is optional to include the COS feature in the Subscriber Service Profile table.

Table 3-2 summarizes how to coordinate provisioning options for COS and OCB.

Table 3-2   Coordination of Provisioning Options Between COS and OCB Features

Feature Included (1) or Excluded (0) in the Service Provisioned for the Subscriber		COS-RESTRICT-ID Included (1) or Excluded (0) in the Subscriber Table for the Subscriber	Features Delivered by the System [1]	How the System Reports Billing Data
OCB Feature	COS Feature			
0	0	0	No restrictions on outgoing calls.	n/a
0	0	1	No restrictions on outgoing calls.	n/a
0	1	0	No restrictions on outgoing calls.	n/a
0	1	1	Full COS functionality. No OCB.	COS
1	0	0	OCB, but without black/white list. No COS.	OCB
1	0	1	OCB with black/white list. To the extent that COS-RESTRICT is configured, additional COS features apply to the subscriber. In this case, OCB treatment takes precedence over COS treatment.	OCB
1	1	0	OCB, but without black/white list. No COS.	OCB
1	1	1	OCB with black/white list. To the extent that COS-RESTRICT is configured, additional COS features apply to the subscriber. In this case, OCB treatment takes precedence over COS treatment.	OCB

1. This description assumes that OCB (if provisioned for the subscriber) has been activated by the subscriber.

Note   For details of the COS feature, see the "Class of Service Restrictions" section on page 3-2.

OCB Feature Interactions (Release 3.2)

The section describes the interactions of OCB with other features.

OCB Interaction with Call Forwarding

The interaction of OCB and call forwarding features depends upon the sequence in which they are activated.

> **Note**   In this section, "CFx" refers to any of the call forwarding features, CFU, CFB, CFNA, or call forwarding combined (CFC).

- If OCB is activated prior to CFx activation—OCB screening is performed on each DN the user enters when attempting to activate CFx. Successful CFx activation depends on the existing OCB K-VALUE and the forward-to DN:
    - If the existing OCB K-VALUE is set to block calls to the forward-to DN, then the system does not allow CFx activation. The user receives an error announcement.
    - If the OCB K-VALUE allows calls to this DN, then the CFx activation process continues. Once the CFx activation attempt to a specific DN is accepted by the system, it is applicable permanently regardless of any future OCB K-VALUE changes. That is, future changes to the OCB K-VALUE have no effect on CFx invocation. CFx to this DN can be deactivated by the user in the normal manner (#XX#).
- If CFx is activated prior to OCB activation—The user can activate the OCB feature, or change the OCB K-VALUE, regardless of the existing CFx feature. However, invocation of OCB depends upon the type of call:
    - User-dialed calls—User-dialed calls can be blocked by OCB (depending on the K-VALUE).
    - Forwarded calls—CFx remains active as originally set up by the user, therefore, calls forwarded by the CFx feature *are not* blocked using OCB screening.

OCB Interaction with COS Restriction

If the OCB is assigned and active on the subscriber line, the COS-RESTRICT-ID is provisioned for the subscriber, and the black/white-list functionality is also provisioned, the subscriber will receive OCB treatment including black/white-list functionality. The system will apply all provisioned COS features to the subscriber, but OCB treatment takes precedence over COS treatment. For more information on coordinating the provisionable features of COS and OCB, see Table 3-2.

> **Note**   The service provider can provision an exception list to override COS and OCB screening on certain types of calls. See the "Exemptions from COS and OCB Restrictions" section on page 3-3.

OCB Enhancements for Release 4.4.1

This section describes the enhancements that have been made in Release 4.4.1 to the basic OCB feature that was introduced in Release 3.2. The Release 3.2 information is available in the "OCB for Release 3.2" section on page 3-16.

OCB Subscription and Provisioning (Release 4.4.1)

The service provider sets up OCB service at the request of the subscriber. There are a number of service provider provisionable parameters that affect the behavior of the feature on the subscriber line:

- Vertical service code (VSC)—ASCII strings that the user must enter to access OCB activation, deactivation, and interrogation options. The recommended values are *54*, #54* and *#54# as used in the examples below. However, VSCs are not preprovisioned in the system. The service provider can provision these values with any valid unique ASCII string up to five characters long.

  > **Note** The valid formats for VSC ASCII strings are listed in the VSC table specification in the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*. The preprovisioned VSC values are listed in the Vertical Service Code appendix of the same document.

- Private identification number (PIN)—A digit string that the user must enter for authorization to set OCB activation and deactivation options from his or her local phone.

  > **Note** Initially, the service provider or the user establishes a PIN for the user. Thereafter, the user cannot modify the PIN.

- PIN length (PIN-LEN)—The number of digits required for a valid PIN (can be provisioned as 1 to 8 digits).

  The PIN and PIN-LEN can be provisioned by the service provider.

  The PIN and PIN-LEN cannot be provisioned or changed by a user via the handset if the OCB-PROFILE has not been provisioned at either the point-of-presence (POP) or at the office level. However, if the OCB-PROFILE has been provisioned and the FREE_SELECT_PIN token has been set to Y (Yes), a subscriber can free-select and register a PIN using a handset at activation if a PIN has not already been assigned and registered.

- Allowed activation/deactivation attempts and lockout parameters—OCB can be provisioned to limit the number of times that a user can enter an incorrect PIN within a specified time. If the limit is exceeded, the system ignores further activation and deactivation attempts for a provisionable length of time (lockout period).

OCB Activation and User Options (Release 4.4.1)

OCB activation (OCBA) allows a user to activate OCB and select various call barring options on the handset (local phone). A user does this by dialing *54*K-VALUE<PIN># (the trailing # is optional to signify the end of the entry). The parameters are defined as follows:

- *54* is the VSC the user enters on the handset to access the OCBA feature.

- K-VALUE is the parameter that determines the type of outgoing calls to be barred. For Release 4.4.1, OCB can enable K-values up to 9 levels.

  > **Note** A K-Value can be mapped to a special mapping table, the OCB-K-Value table.

- <PIN> is the assigned private digit string that the user must enter. A success announcement is given on a successful activation, and an error announcement, indicating the type of error, is given if activation is unsuccessful.

> ✎ **Note**   The K-VALUE can be changed when the OCB feature is active if the subscriber performs another activation and enters a different value for the K-VALUE token. The new K value overwrites the preceding K value.

If a user enters an incorrect PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning (Release 4.4.1)" section on page 3-21.

The following user actions are invalid, and the system provides an appropriate error announcement:

- The user enters a value for K-VALUE that is not in the range 1 through MAX-K-VALUES (as specified in the OCB-PROFILE table).

  If a subscriber attempts an activation and specifies a K-VALUE that is not in the range established by the provisioned MAX-K-VALUE token, the subscriber receives an error announcement. If the MAX-K-VALUES token is not provisioned in the OCB-PROFILE table at either the POP or Cisco BTS 10200 Softswitch, by default, the valid K-VALUE range is 1 through 3.

> ✎ **Note**   The POP table is checked first for the MAX-K-VALUE and then the office level (call agent configuration table). If the token is not provisioned in either table, OCB defaults to the behavior established in the initial release of OCB in Cisco BTS 10200 Release 3.2.

- The user is not provisioned for the OCB feature.
- The user enters an incorrect PIN.

OCB Deactivation (Release 4.4.1)

The Enhanced OCB feature supports three options for OCB deactivation. An option is specified by provisioning the DEACTIVATION-OPTION token in the OCB-PROFILE table.

NO-K-VALUE Option

To select the NO_K_VALUE deactivation option, the subscriber enters <VSC><PIN> without entering a K-VALUE.

K-VALUE-NO-MATCH Option

The K-VALUE-NO-MATCH deactivation option enables a user to deactivate all OCB on the handset. The user does this by dialing #54*K-VALUE<PIN>#. The parameters are defined as follows:

- #54* is the VSC the user enters on the handset to access the OCBD feature
- K-VALUE must be entered as a value from 1 through MAX-K-VALUES. However, the actual value is ignored during processing.
- <PIN> is the same as for OCBA.

> ✎ **Note**   If the K-VALUE token is not provisioned in the OCB-K-VALUE table at either the POP or softswitch, by default, the K-value range is 1 through 3.

K-VALUE-MATCH

The K-VALUE-MATCH deactivation option requires the subscriber to enter a K-VALUE that matches the K-VALUE provisioned for the subscriber. If the subscriber enters a K-VALUE that does not match the value provisioned for K-VALUE, the subscriber receives an error announcement.

A success announcement is given on a successful deactivation, and an error announcement, indicating the type of error, is given if deactivation is unsuccessful.

> ✎
> **Note**   Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for provisioning details.

If a user enters an incorrect PIN repeatedly in a specified time period, the system can lock out further activation or deactivation attempts, as described in the "OCB Subscription and Provisioning (Release 4.4.1)" section on page 3-21.

OCB Interrogation (Release 4.4.1)

OCB interrogation for Release 4.4.1 operates as it did for Release 3.2.

OCB Invocation and Screening (Release 4.4.1)

For a calling party that is subscribed to OCB, and has activated the feature, OCB is invoked for every call made after the called party digits are dialed.

OCB Lockout Behavior (Release 4.4.1)

The LOCK-OUT, TIME-OUT, and FAIL-CNT tokens in the OCB-PROFILE and FEATURE tables are intended to prevent unauthorized changes or bypassing of OCB screening. If a user repeatedly enters the PIN incorrectly on the handset, the system can lock the line against both OCBA and OCBD.

- For the Enhanced OCB feature, if the FAIL-CNT (fail count), LOCK-OUT, and TIME-OUT tokens are provisioned in the OCB-PROFILE table, OCB lockout behaves according to those specifications.

- If the OCB-PROFILE table is not provisioned, OCB lockout behaves according to the provisioning of the LOCK-OUT, TIME-OUT, and FAIL-CNT tokens in the FEATURE table.

The tokens control the lockout behavior as described in Table 3-3.

> 🔍
> **Tip**   Note that there is no service lockout when either the TIME-OUT or FAIL-CNT token is set to zero.

Table 3-3   OCB Lockout Behavior

OCB Tokens in Feature Table			Lockout Behavior Due to OCBA/OCBD Misuse
LOCK-OUT	**TO**	**FAIL-CNT**	
n/a	n/a	0	No service lockout
n/a	0	n/a	No service lockout
0	1 or greater	1 or greater	OCBA and OCBD are locked out indefinitely after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes
1 or greater	1 or greater	1 or greater	OCBA and OCBD are locked out for <LOCK-OUT> minutes after the user misuses the OCBA/OCBD feature <FAIL-CNT> times in <TO> minutes

OCB Feature Interactions (Release 4.4.1)

OCB feature interactions for Release 4.4.1 are the same as for Release 3.2.

Limitations and Restrictions (Release 4.4.1)

This section provides information on limitations and restrictions that apply to the enhanced OCB feature for Release 4.4.1.

Limitations On Reporting of Traffic Counters (Release 4.4.1)

Cisco BTS 10200 Softswitch OCB does not support the following traffic counters whenever it uses the OCB-Profile to block calls:

- POTS_OCB_LOCAL_BLOCKED
- POTS_OCB_NATL_BLOCKED
- POTS_OCB_INTL_BLOCKED

Special Call Types (Release 4.4.1)

Emergency calls (calls with call-type=EMG) are never subject to COS and OCB screening. The system always exempts emergency calls from COS and OCB screening without considering any provisioned parameters. Note that for Release 4.5.x and later it is possible to provision AMBULANCE, FIRE, and POLICE as subtypes of EMG in the Destination table. If provisioned as subtypes of EMG, these types are given the same treatment as EMG.

SIP Subscribers (Release 4.4.1)

If the service provider sets NANP_DIAL_PLAN="Y" in the dial plan for a SIP subscriber, the OCB feature will not operate properly.