

Tenor CDR Description

October 8, 2002

This document may contain information that is proprietary and confidential to Quintum Technologies, Inc., its partners, VARs and/or customers. This document may not be duplicated or shown to any party or parties other than those that are named within this document or authorized by Quintum Technologies, Inc.

This document may not be shown to any competing vendors or VARs without Quintum Technologies, Inc., written consent.



- I. Overview 3
- II. Establishing a Connection to the CDR Ports of the Tenor..... 4
- III. Tenor Related Configuration Commands..... 5
 - _Toc25722324
 - CDR Server Establishes Connection with Tenor..... 6
 - Using Telnet to Access CDR Records 6
- IV. CDR Output Format. 8
 - Sample CDR Record - Standard format (cdrformat = 0 or 100) 8
 - Sample CDR Record: Extended Format (cdrformat set to "1" or "101")..... 8
 - CDR Field Definitions: "Standard Format" Fields (*Settings 0 & 100*) 8
 - CDR Field Definitions: "Extended Format" Fields (*Settings 1 & 101*)..... 9
- V. Command Quick List 10
 - Sys Commands (config sys#)..... 10
 - Radius Commands (config rad user#). 11
- VI. Common Alarms and Conditions 11
 - Common Alarms 11
 - Call Event(s) Lost 11
 - Conditions for Troubleshooting..... 11
 - 1. 1111*as Called Number 11
 - 2. No remote IP address in CDR record..... 12
 - 3. Disconnect Cause Code 34 12
 - 4. Disconnect Cause Code 16..... 12
 - 5. Not able to access the CDR port from Telnet. 12
- VII. Appendix - Disconnect Cause Codes..... 13

I. Overview.

Through the Call Detail Recording (CDR) feature, Tenor is able to generate a CDR at the completion of each call, including a multi-session IVR call. A CDR is a string of data which contains call information such as call date and time, call length, calling party, called party, etc. From this information you can capture billing type data, which can be used to create billing reports.

The Tenor will store up to 1500 CDR records. However, this buffer is shared for both CDR and Radius records (if Radius is used). For a given application or call, there could be more than one record. For example, if you are using a Radius Server for pre-paid calling card services, there could be several radius messages stored in the buffer which will use up space a decrease the number of CDR records to be stored. Each Radius record uses one CDR record space.

Without Radius Server applications, there will be one CDR record generated for each call.

The CDR Buffer is a circular buffer, this means that any number of CDRs over 1500 will overwrite the existing CDRs). We advise that you set up a PC or workstation to act as a CDR server responsible for receiving the CDRs as they are generated (up to 2 servers can be set up to collect CDRs from Tenor). The server will be responsible for capturing CDRs via TCP/IP, processing/storing them in permanent memory, and producing billing records.

NOTE:

If the Tenor loses power either due to a power outage or to a manually initiated power off and on, all CDR records in the buffer will be lost, the records id will be set to 1 and the session id will be reset to 1. If the Tenor is reset via software, then it will not lose these records.

The `cdrformat` (more information below) configuration parameter command is used to choose which of the two (2) possible Call Data Records output formats (Standard or Extended) you would like sent to your CDR Server from the Tenor.

In addition, there is an option to have the CDR Server and the Tenor “synchronize”. This is done by way of using a unique Session ID number to confirm that neither unit has been reset, or has been “power cycled”, and that the Tenor has delivered all call records to the CDR Server.

In software version P4-2-14, the feature of using both the CDR server and a Radius was disabled. In this release if you had the **accountingtype** (under config radius user#) set to 1 or 2, then you could not collect records from the CDR ports.

In software version P4-2-16 or higher, this feature has been re-introduced and enhanced to support multi-session IVR/Radius calls. However, the record buffer size of 1500 will still remain and each IVR session may use multiple records thereby reducing the number of complete sessions stored in the buffer.

The CDR Server Software is 3rd party software and is not provided by Quintum.

II. Establishing a Connection to the CDR Ports of the Tenor.

In order to capture the CDR records, you must establish a connection to the Tenor's CDR ports. This can be done either through a standard Telnet, or through the use of a CDR server program (user provided). It does not matter which you use at the connection flow will be the same.

Additionally, it does not matter which end initiates the connection, the flow will be the same.

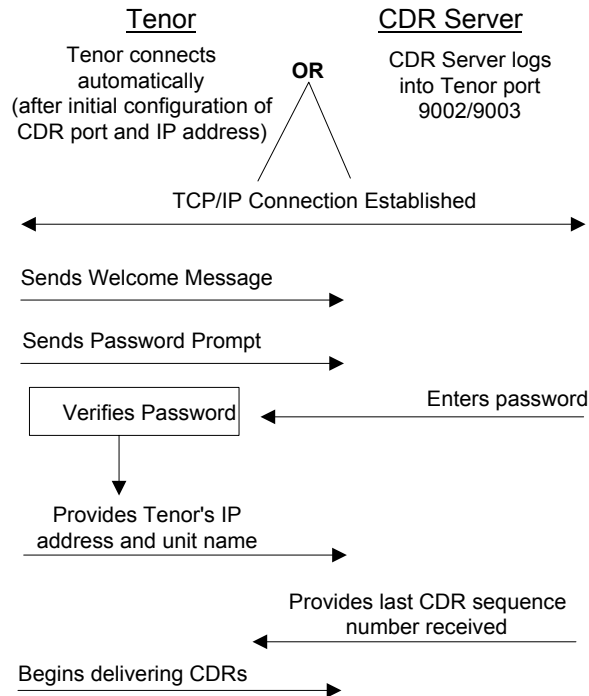
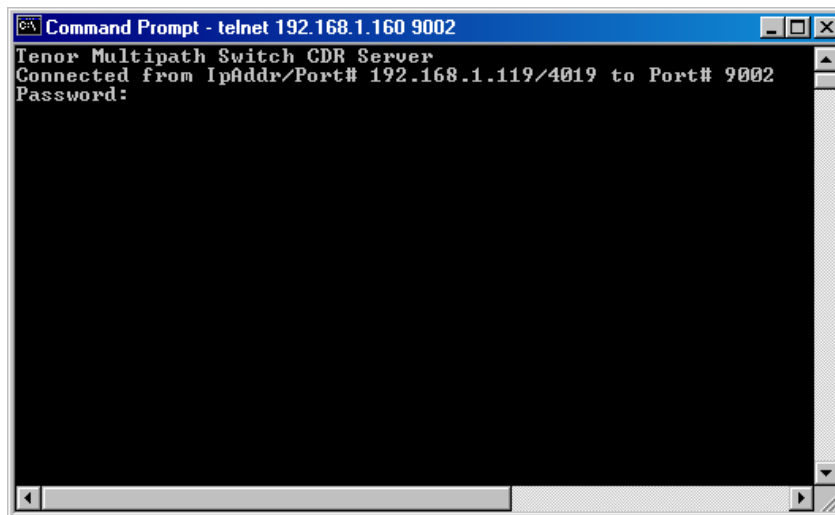


Figure 1

Once the TCP/IP connection is established, the Tenor will provide a Welcome message as shown below;



```

Command Prompt - telnet 192.168.1.160 9002
Tenor Multipath Switch CDR Server
Connected from IpAddr/Port# 192.168.1.119/4019 to Port# 9002
Password:
    
```

Figure 2

At this point, you must enter the CDR password, if one has been configured in the Tenors configuration, and hit enter. Once you are logged in you will get the following display;

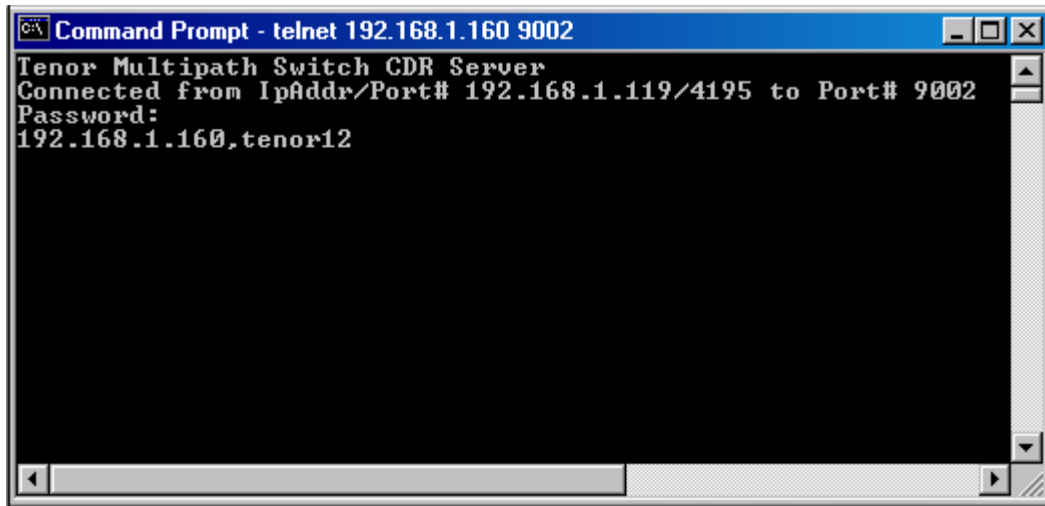


Figure 3

This will provide you the IP address and unit name for this Tenor. Now the Tenor is waiting for an input from you or your CDR server. You must tell the Tenor what record to start providing to you. If you just hit enter, the Tenor will provide all the records in its buffer, up to 2000. You or your CDR server can optionally enter the record id of the last record you received and then the Tenor will only provide the records it has from that id forward.

III. Tenor Related Configuration Commands.

Before attempting to collect CDRs, you should configure the desired information. Through CLI commands under the “sys” Prompt Level, you can determine the appropriate output format, assign CDR Server IP Address, CDR Server Port Number, and CDR Server Password information using the following CLI commands: *cdrserverip*, *cdserverport*, *cdrformat* and *cdrpassword*.

- cdrformat* This configuration parameter command is used to choose which of the two (2) possible Call Data Records output formats you would like sent to your CDR Server. (See below)
- cdrserverip*: IP addresses of the CDR server. (Used when Tenor establishes connection with CDR Server.)
- cdserverport*: The port numbers used by the CDR server(s). (Used when Tenor establishes connection with CDR server.)
- cdrpassword*: Password to be used by the CDR server(s) to gain permission to access the Tenor.



On Both The Analog & Digital Tenor, The “CDRFORMAT” parameter settings are as follows:
config sys# cdrformat {x}

Setting Description

0	Gives the standard CDR output (See next page for output details)
1	Gives the extended CDR output. (See next page for output details)
100	Same data as Selection 0, but adds the Session ID functionality.
101	Same data stream as Selection 1, but adds the Session ID functionality.

Tenor Establishes Connection with CDR Server

To capture CDR reports via CDR server (i.e., a PC or workstation you use to capture CDR data) you must first assign configure the IP address and port number of the CDR server in Tenor (see CLI commands in previous section). Once these are configured, Tenor will be able to establish a TCP/IP session with the server on its own. The Tenor will initiate this connection to your CDR server every 5 minutes and not after each call is completed.

Once you have a port configured in the Tenor for this using the *cdrserverip* and *cdrserverport* commands, then that port becomes unavailable for any other use and you will not be able to telnet to this port. For example, if you set port 9002 for the CDRServer in the Tenor configuration, then you will not be able to access port 9002 via telnet or any other means as the Tenor will reserve this strictly for the delivery of CDRs to the configured IP address.

CDR Server Establishes Connection with Tenor

If no IP address/port number is configured via CLI (see previous section), the CDR server has to initiate the session. Tenor uses TCP port numbers 9002 and 9003 on its side for the CDR sessions. This is also how you would telnet to the Tenor to access the CDR records.

Whether Tenor establishes the connection with the CDR server or the CDR server attempts to establish the connection, there is a limit of 5 attempts to enter the correct password before the TCP session is terminated (to configure a password, see the CLI command *cdrpassword* in the previous section).

After the CDR server successfully logs into the CDR port of Tenor, the CDR server will be provided with the IP address and unit name of the Tenor. The CDR server will then supply the sequence number of the last CDR that it has received from Tenor. If the last CDR number is unknown, the server should send 0 for the sequence number. After this exchange, the Tenor will start delivering new CDRs to the server.

Using Telnet to Access CDR Records

Optionally, you can use a standard Telnet session to connect to the Tenor’s CDR ports and look at or capture the CDR records. Keep in mind that if you have the Tenor configured to deliver the CDR records to a CDR server using one of the 2 ports, you cannot telnet to the port configured.

Telnet software differs from vendor to vendor. Additionally, the standard Telnet that Microsoft provides is different from Windows 98 to 2000 to NT, etc. You will need to check



your Telnet program help screen or with the Telnet software vendor for specific information on how to use the Telnet session.

In order to use Telnet to connect to the Tenor's CDR port, you must be able to specify the Tenor's IP address and the CDR port (either 9002 or 9003) within the Telnet session. Check with your Telnet software to see how this is done. From Windows, if you open a DOS window and type "telnet xxx.xxx.xxx.xxx 900y" (xxx.xxx.xxx.xxx = IP address of Tenor, 900y = either 9002 or 9003), then you will be connected to the appropriate CDR port.

Once you are connected, the call flow is the same as if you are a CDR server. The Tenor will ask you for the CDR password. If you have previously configured this, you must now enter the password. If you have not configured one, you may hit enter.

At this point, you MUST setup to capture a log file if you want to put the records to a file for use later on. Each version of Telnet and each vendor of Telnet has a different way of enabling a log file. Check with your software on how to start a log file to capture everything that happens on the screen to a text file.

Once you have enabled a log file and specified the location and name of this file you can continue. You can now either just hit enter and the Tenor will provide all of the CDR records in its buffer (up to 2000 records), or if you have previously received CDR records, and you know the record id of the last record you previously received, you can type this number in and the Tenor will only provide the records from that point forward.

Once the Tenor has completed providing the CDR records, stop the log file and then you can close this window. Now you have a text file of the CDR records and you can import this to Excel or Lotus or any other spreadsheet or database or any other program that allows you to import information from any text file. Keep in mind that the fields are comma delimited and that you should have the cells setup for text.

L	1	Call Number Type.	The called numbering plan used for the call per Q.931. Possible common entries are as follows: 1 = Public/E.164, 9 = Private.
M	1	Incoming Line.	If the call is incoming, this field identifies which line the call came in on. Valid entry: 1 = PBX, 2 = PSTN. This field will be empty if the call is an incoming VoIP call.
N	1	incoming Channel.	If the call is incoming, this field identifies which channel the call came in on. Valid entry: 1-31. This field will be empty if the call is an incoming VoIP call.
O	1	Outgoing Line.	If the call is outgoing, this field identifies which line the call is going out on. Valid entry: 1 = PBX, 2 = PSTN. This field will be empty if the call is an outgoing VoIP call.
P	1	Outgoing Channel.	If the call is outgoing, this field identifies which channel the call went out on. Valid entry: 1-31. This field will be empty if the call is an outgoing VoIP call.
Q	null	Auto Switch Time.	This is the date and time the AutoSwitch occurred (when the call is switched from VoIP to circuit). The entry will be in the following format: <code>yyyymmddhhmmss</code> where <code>yyyy</code> (4 digits for year), <code>mm</code> (2 digits for month), <code>dd</code> (2 digits for day), <code>hh</code> (2 digits for hour), <code>mm</code> (2 digits for minutes), <code>ss</code> (2 digits for seconds). If an AutoSwitch did not occur, this field will be blank.
R	null	Auto Switch Duration.	The number of seconds that the AutoSwitch call was active. Valid entry: <code>xx</code> .
S	0	Bad IP Quality Events.	The number of bad quality events that occur during a VoIP call. This number determines the overall quality of a call.
T	0	Auto Switch Flag.	The terminating side of the AutoSwitch call initially terminates to the internal AutoSwitch agent before the call is actually autoswitched. This termination generates an extra CDR in addition to the original call that is autoswitched. This field identifies a call that is terminated to the AutoSwitch agent. 0 = normal call, 1 = termination to the AutoSwitch agent.

CDR Field Definitions: "Extended Format" Fields (Settings 1 & 101)

Includes all "Standard Format" Fields **plus**:

U	14155551000	Calling Party Number	The Number called from. The format will be delivered in whatever format the PSTN or PBX delivers to the Tenor. It will not necessarily be in International format.
V	12345678901234	PIN Code	PIN Code entered. 14 digits maximum. This field will be blank if a PIN is not configured.
W	0123456789	Local Call ID #	Unique identification number, generated by the local-side Tenor, for call record matching purposes. Generated for all calls. **
X	9876543210	Remote Call ID #	Unique identification number, generated by the remote-side Tenor, for call record matching purposes. Only generated for IP calls. **

** - For a given IP call, Local Call ID in the CDR of one Tenor should match the Remote Call Id in the CDR of the other Tenor. If the call is to or from a non-Quintum unit, then the Remote Call Id will be blank.

V. Command Quick List

This section will provide a quick list of the commands presented earlier.

Sys Commands (config sys#)

cdrserverip

Description: Used to set up to 2 IP address of PC's that are running CDR Server Collection Programs. When configured, the Tenor will initiate a connection to the specified CDR Servers every 5 minutes.

Prompt Level: config sys#

Syntax: **cdrserverip** {1 | 2} {*ipaddr*}

Arguments: **1** Selects the 1st CDR server position in the Tenor configuration.
2 Selects the 2nd CDR server position in the Tenor configuration.
ipaddr IP address that is the CDR Server for this position.

Settings: None.

Default: 0.0.0.0

Availability: All Tenor Releases.

Guidelines: To disable or delete a CDR server, enter 0.0.0.0 after the corresponding position.

Example: config sys# **cdrserverip 1 192.168.1.10** (sets the first CDR server to 192.168.1.10)
 config sys# **cdrserverip 2 192.168.1.15** (sets the second CDR server to 192.168.1.15).
 config sys# **cdrserverip 2 0.0.0.0** (Deletes the 2nd CDR server IP address).

cdrserverport

Description: Used to assign which port (9002 or 9003) is to be used for the associated CDR server from the Tenor.

Prompt Level: config sys#

Syntax: **cdrserverport** {1 | 2} {*port*}

Arguments: **1** Selects the 1st CDR server position in the Tenor configuration.
2 Selects the 2nd CDR server position in the Tenor configuration.
port Tenor port (9002 or 9003) that will be used for this CDR server.

Settings: None.

Default: 0000

Availability: All Tenor Releases.

Guidelines: To disable or delete a CDR server, set the corresponding cdrserverip to 0.0.0.0. You may use the same port for both cdrservers 1 & 2. Whatever port you configure, once you submit, this port will not allow a connection to it from an external device. It will only initiate connections out.

Example: config sys# **cdrserverport 1 9002** (sets the first CDR server port to 9002)
 config sys# **cdrserverport 2 9002** (sets the second CDR server port to 9002)

cdrformat

Description: Used to set the format for the CDR output to the CDR Servers.

Prompt Level: config sys#

Syntax: **cdrformat** {0 | 1 | 100 | 101}

Arguments: **0** Provides the standard CDR output format as explained earlier.
1 Provides the standard CDR output **plus** the extended information.
100 Provides the same data as option 0, but adds the Session Id.
101 Provides the same data as option 1, but adds the Session Id.

Settings: None.

Default: 0

Availability: All Tenor Releases.

Guidelines: None

Example: config sys# **cdrformat 1** (sets the CDR format to the extended version).
config sys# **cdrformat 100** (sets the CDR format to the standard with session id).

cdrpassword

Description: Used to set a password for access to the CDR ports.
Prompt Level: config sys#
Syntax: **cdrpassword** or **cdrpass {password}**
Arguments: **password** Any alphanumeric entry that will be the password for access to the CDR ports. No spaces allowed.
Settings: None.
Default: null
Availability: All Tenor Releases.
Guidelines: None
Example: config sys# **cdrpass 1234** (sets the CDR password to 1234).
config sys# **cdrpass** (deletes the cdr password).

Radius Commands (config rad user#).

accountingtype

Description: Used to set the accounting method for delivering CDR information to a Radius Server.
Prompt Level: config rad user#
Syntax: **accountingtype** or **accountingt [0 | 1 | 2]**
Arguments: **0** No accounting record will be sent to the Radius Server
1 Only 1 accounting message (for the incoming leg of call) to the Radius.
2 Send 2 accounting messages (one for each leg of the call) to the Radius.
Settings: None.
Default: Null
Availability: All Tenor Releases.
Guidelines: Must have a valid Radius Server setup and the IP address of the Radius Server configured in the Host IP parameter.
Example: config rad user# **accountingtyp 2**

VI. Common Alarms and Conditions

Common Alarms

The following alarms may be observed in conjunction with these changes.

Call Event(s) Lost

This indicates that the Tenor CDR buffer is full and that new CDR records have overwritten older records in the buffer.

Conditions for Troubleshooting

*1. 1111*as Called Number*

This indicates that a call was received to the Tenor's built-in IVR from the PSTN of the Tenor. This could be for a 2nd dial tone or for a Radius call. The number 1111* is used internally for the Tenor to route the call to the IVR (2nd dial tone or voice prompt for Radius) and will be shown if the user hangs up the phone before dialing a destination number.



2. *No remote IP address in CDR record.*

This can be for many reasons. The first is that, like condition 1 above, the user did not dial a destination number, but instead, disconnected the line. Therefore the Tenor did not route the call to any location. Another reason is that the call went from PSTN to PBX or PBX to PSTN. You can verify this by checking both the incoming line/channel and outgoing line/channel.

3. *Disconnect Cause Code 34.*

This means that a call was attempted, but there was no available channel to terminate the call to. This usually happens when you are over-subscribing the destination unit. In the case where a Tenor is the termination unit, if it is an 8 port unit (A800), and there are 8 calls active on it already, any additional calls sent to it will get this cause code 34. Many times, a Cisco will be incorrectly configured and send more calls to the end unit than it could handle. Additionally, if the Tenor is in between a PBX and PSTN, it is highly possible that there could be no more channels available if the site experiences peak periods where many calls come from the PSTN and pass through to the PBX locally (or vice-versa). There could be other reasons for this, but the customer should check this first.

4. *Disconnect Cause Code 16.*

This indicates a normal call clearing, but has generally happened prior to the call be connected as if the call connected, there would be no disconnect cause code. This can happen for many reasons, such as the person heard a busy tone and in analog units, the busy tone may not be translated to the cause code for user busy (17). This could also indicate a problem with voice quality or getting voice in one direction only. The customer should perform test calls in this case to address the problem.

5. *Not able to access the CDR port from Telnet.*

When you try to telnet to one of the CDR ports on the Tenor, you do not get a connection to the CDR port. This happens when either someone else is already logged in to this port or you have configured this port for use as one of the 2 CDR Server ports in the `config sys# cdrserverport` commands. Unlike normal telnet, if someone is already connected to the CDR server port you are trying to access, you will not be able to connect to it until the other person disconnects. Additionally, if the Tenor is configured with this port as the CDR server port, as mentioned above, then the Tenor will not allow anyone to access this port. Change the configuration of this to a different port or delete it out of the configuration all-together.

VII. Appendix – Disconnect Cause Codes

The following is a complete list of Cause Codes based on the Q.931 specification. Not all of these codes may be applicable in all situations;

Decimal Value	Hexadecimal Value	Definition
1	01	Unallocated (unassigned) number. This number is not in the routing table or it has no path across the ISDN cloud (network). 1. Check routing table to see if the number is available. 2. Check to make sure the correct digits were dialed and it is a valid number.
2	02	No route to specified transit network (national use). The number was dialed with a transit network code such as 108880 to from AT&T to MCI and there is no route between the 2 networks.
3	03	No route to destination. The dialed number is in the routing plan, but there is no physical route to the destination. 1. The link may be down at one end or the other. 2. The span or WAN is not connected correctly.
4	04	Send special information tone. Indicates that the called party cannot be reached for reasons that are of a long-term nature and that the special information tone should be returned to the calling party.
5	05	Misdialed trunk prefix (national use). Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	06	Channel Unacceptable. Indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.
7	07	Call awarded and being delivered in an Established channel. Indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for similar calls (e.g. packet-mode virtual calls).
8	08	Pre-Emption. Indicates that the call is being pre-empted.
0	09	Pre-Emption – Circuit reserved for reuse. Indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.
16	10	Normal Call Clearing. This is one of the most common cause codes and is received for many reasons. It usually occurs because someone hung up the call at one side or the other.
17	11	User Busy. The number dialed is busy and cannot receive any more calls.
18	12	No User Responding. The called party does not respond to the call, or does not wish to answer the call.
19	13	No Answer from User (User Alerted). The called party has been alerted to the incoming call, but does not respond with a connect indication within a prescribed period of time. NOTE: This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.

20	14	<p>Subscriber Absent.</p> <p>Used when a mobile station has logged off, radio contact is not obtained with a mobile station or if a personal telecommunications user is temporarily not addressable at any user-network interface.</p>
21	15	<p>Call Rejected.</p> <p>Indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.</p> <p>May also be generated by the network, indicating that the call was cleared due to a supplementary service constraint.</p>
22	16	<p>Number Changed.</p> <p>This is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause value, cause number 1 shall be used.</p>
26	1A	<p>Non-Selected User Clearing.</p> <p>Indicates that the user has not been awarded the incoming call.</p>
27	1B	<p>Destination Out-of-Order.</p> <p>This is a working number, but the span to the destination is not active or there is a problem sending messages to this destination.</p>
28	1C	<p>Invalid Number Format (address incomplete).</p> <p>Indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete. This can happen when you are calling out using a network type number (enterprise) when you should be calling out Unknown or National for the Type of Number (TON).</p>
29	1D	<p>Facility Rejected.</p> <p>This cause is returned when a supplementary service requested by the user cannot be provided by the network.</p>
30	1E	<p>Response to STATUS ENQUIRY.</p> <p>This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.</p>
31	1F	<p>Normal, Unspecified.</p> <p>This is a very common cause code and happens when the network is not able to determine what to do with the call being made.</p>
34	22	<p>No Circuit/Channel Available.</p> <p>There are no channels available to handle this call. This may happen if the destination gateway is full with calls.</p>
38	26	<p>Network Out-of-Order.</p> <p>Indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time.</p>
39	27	<p>Permanent Frame Mode Connection Out-of-Service.</p> <p>This cause is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service.</p>
40	28	<p>Permanent Frame Mode Connection Operational.</p> <p>This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information.</p>
41	29	<p>Temporary Failure.</p> <p>The call was disconnected due to a network failure.</p> <p>The network is not functioning correctly and that the condition is not likely to last a long period of time; e.g. the user may wish to try another call attempt almost immediately.</p>

42	2A	<p>Switching Equipment Congestion.</p> <p>Indicates that the switching equipment generating this cause is experiencing a period of high traffic.</p>
43	2B	<p>Access Information Discarded.</p> <p>Indicates that the network could not deliver access information to the remote user as requested, i.e. user-to-user information, low layer compatibility, high layer compatibility, or sub-address, as indicated in the diagnostic.</p>
44	2C	<p>Requested Circuit/Channel not Available.</p> <p>This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.</p> <p>This may happen when you get in a glare condition: Both sides are selected top-down or bottom-up channel hunting.</p>
47	2F	<p>Resource Unavailable, Unspecified.</p> <p>Used to report a resource unavailable event only when no other cause in the resource unavailable class applies.</p>
49	31	<p>Quality of Service Not Available.</p> <p>Used to report that the requested Quality of Service, as defined in Recommendation X.213, cannot be provided (e.g. throughput or transit delay cannot be supported).</p>
50	32	<p>Requested Facility Not Subscribed.</p> <p>This cause indicates that the user has requested a supplementary service which is implemented by the equipment which generated this cause, but the user is not authorized to use.</p>
53	35	<p>Outgoing Calls Barred Within Closed User Group (CUG).</p> <p>Indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.</p>
55	37	<p>Incoming Calls Barred within CUG.</p> <p>Indicates that although the called party is a member of the CUG for the incoming CUG call, incoming calls are not allowed to this member of the CUG.</p>
57	39	<p>Bearer Capability Not Authorized.</p> <p>Indicates that the user has requested a bearer capability which is implemented by the equipment, which generated this cause but the user is not authorized to use.</p>
58	3A	<p>Bearer Capability Not Presently Available.</p> <p>Indicates that the user has requested a bearer capability, which is implemented by the equipment which generated this cause but which is not available at this time.</p>
62	3E	<p>Inconsistency in Designated Outgoing Access Information and Subscriber Class.</p> <p>This cause indicates that there is an inconsistency in the designated outgoing access information and subscriber class.</p>
63	3F	<p>Service or Option Not Available, Unspecified.</p> <p>Used to report a service or option not available event only when no other cause in the service or option not available class applies.</p>
65	41	<p>Bearer Capability Not Implemented.</p> <p>Indicates that the equipment sending this cause does not support the bearer capability requested (i.e. requesting 64kb data when only speech is supported).</p>
66	42	<p>Channel Type Not Implemented.</p> <p>Indicates that the equipment sending this cause does not support the channel type requested.</p>
69	45	<p>Requested Facility Not Implemented.</p> <p>Indicates that the equipment sending this cause does not support the requested supplementary service.</p>

70	46	<p>Only Restricted Digital Information Bearer Capability is Available (national use).</p> <p>Indicates that the calling party has requested an unrestricted (64kb) bearer service but that the equipment sending this cause only supports the restricted version of the requested bearer capability.</p>
79	4F	<p>Service or Option Not Implemented, Unspecified.</p> <p>Used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.</p>
81	51	<p>Invalid Call Reference Value.</p> <p>Indicates that the equipment sending this cause has received a message with a call reference which is not currently in use or assigned on the user-network interface. E.G. The call that is being reference by this value, does not exist on this system.</p>
82	52	<p>Identified Channel Does Not Exist.</p> <p>Indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call.</p> <p>For example, if a user has subscribed to those channels on a PRI numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.</p>
83	53	<p>A Suspended Call Exists, but This Call Identity Does Not.</p> <p>Indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended calls(s).</p>
84	54	<p>Call Identity in Use.</p> <p>Indicates that the network has received a call suspended request containing a call identity which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.</p>
85	55	<p>No Call Suspended.</p> <p>Indicates that the network has received a call resume request containing a call identity information element, which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.</p>
86	56	<p>Call Having the Requested Call Identity Has Been Cleared.</p> <p>Indicates that the network has received a call resume request containing a call identity information element indicating a suspended call that has in the meantime been cleared while suspended.</p>
87	57	<p>User Not Member of CUG.</p> <p>Indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.</p>
88	58	<p>Incompatible Destination.</p> <p>The number being dialed is not capable of the type of call.</p> <ol style="list-style-type: none"> 1. Calling a restricted line in unrestricted mode. 2. Calling a pots phone using unrestricted mode. <p>Indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes which cannot be accommodated.</p>
90	5A	<p>Non-Existent CUG.</p> <p>Indicates that the specified CUG does not exist.</p>
91	5B	<p>Invalid Transit Network Selection (national use).</p> <p>Indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931.</p>
95	5F	<p>Invalid Message, Unspecified.</p> <p>Used to report an invalid message event only when no other cause in the invalid message class applies.</p>

96	60	<p>Mandatory Information Element is Missing.</p> <p>Indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message.</p>
97	61	<p>Message Type Non-Existent or Not Implemented.</p> <p>Indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.</p>
98	62	<p>Message is Not Compatible with the Call State, or the Message Type is Non-Existent or Not Implemented.</p> <p>Indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.</p>
99	63	<p>An Information Element or Parameter Does Not Exist or is Not Implemented.</p> <p>Indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element identifier(s)/parameter name(s) are not defined or are defined but not implemented by the equipment sending the cause.</p>
100	64	<p>Invalid Information Element Contents.</p> <p>The call has an information element that is not understood by the switch being called. This cause is usually followed by the information element that is causing the problem.</p>
101	65	<p>The Message is Not Compatible with the Call State.</p> <p>Indicates that a message has been received which is incompatible with the current call state for this call.</p>
102	66	<p>Recovery on Timer Expired.</p> <p>This occurs when ISDN messages don't arrive in specified time according to the Q.931 specification. This cause is sometimes followed by the timer that has expired.</p>
103	67	<p>Parameter Non-Existent or Not Implemented – Passed On (national use).</p> <p>Indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending the cause.</p>
110	6E	<p>Message with Unrecognized Parameter Discarded.</p> <p>Indicates that the equipment sending this cause has discarded a received message, which includes a parameter that is not recognized.</p>
111	6F	<p>Protocol Error, Unspecified.</p> <p>Used to report a protocol error event only when no other cause in the protocol error class applies.</p>
127	7F	<p>Interworking, Unspecified.</p> <p>Indicates that there has been interworking with a network which does not provide causes for actions it takes. Thus, the precise cause for a message which is being sent cannot be ascertained.</p>