NIS-S227-1

DMS-100 Family

Centrex IP Services

Network Interface Specification

NA012 Issue 01.02 September 1999

NORTEL
NETWORKS™

DMS-100 Family

Centrex IP Services

Network Interface Specification

Publication number:	NIS-S227-1
Document status:	STANDARD
Document release:	Issue 01.02
Issue date:	September 1999
Security status:	Public

Printed in United States of America.

Information subject to change without notice.

Publication History

Date	Issue	Rating
30 September 1999	Issue 01.02	STANDARD

Note 1: Issues rated “Draft” or “Preliminary” are identified alphabetically, in sequence; issues rated “Standard” are identified numerically, in sequence. The issue and date appear on each page of this document.

Note 2: Significant changes and additions are marked with vertical bars in the outer page margins beside the changed or added information.

NOTICE

This specification is provided as a guide for network planners and suppliers of systems and equipment designed to meet the requirements of Nortel Networks Internet Telephony Service specifications. Nortel Networks reserves the right to revise the contents of this guide for any reason, including, but not limited to, conformity with standards promulgated by any public standards agency, advances in technology, or to reflect changes in requirements of communication networks, systems or applications. The provision of any capabilities described in this document is dependent on certain business decisions, resolution of which may also result in changes to, withdrawal of, or addition to, any or all of the capabilities herein.

Nortel Networks makes no representation in respect to and does not warrant any of the information in this Specification, but furnishes such in good faith and to the best of its knowledge and ability. Without restricting the generality of the foregoing, Nortel Networks makes no representations or warranties as to fitness for a particular purpose, or as to whether or not the use of the information in the Specification may infringe any patent or other rights of any other person. The recipient waives any claims it may have against Nortel Networks in respect of any use that the recipient makes of the information or products derived therefrom.

It is expected this Specification will be revised in the future to reflect domestic and international standards as they evolve and DMS-100 service and feature enhancements. Nortel Networks reserves the right to alter or modify this Specification or the equipment to which it relates at any time without notice and without liability.

It is the intent of Nortel Networks to make submissions to standards bodies and adopt domestic and international standards. The contributions currently being discussed at ECSA T1 committees, ITU study groups, and in respect of Bellcore Technical Requirements and Generic Requirements are monitored and incorporated into future programs whenever appropriate.

To order the latest version or additional copies of this document, DMS-100 Internet Telephony Services Network Interface Specification, NIS-S227-1,you may call 1-800-684-2273 from 8:00 AM to 5:00 PM Eastern Time.

Outside of these hours this line will be served by voice mail, or you may write to:

Nortel Networks, Inc.
Merchandise Ordering Specialist
Dept. 6611
P.O. Box 13010
Research Triangle Park, NC 27709

Chapter 1: Introduction

This publication of NIS-S227-1, Issue 01.02 represents Nortel Networks implementation of Centrex IP Services based on the H.323 and H.225.0 Recommendations of the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T). To achieve full compliance with those Recommendations, terminal vendors are advised to build to the original source documents. Terminals built to those Recommendations will be functional on the DMS-100, however, building to NIS-S227-1, Issue 01.02, provides terminals with ITU-T compliance and additional functionality as offered by the DMS-100.

All pages in this issue of NIS-S227-1 are numbered sequentially.

1.1 Introduction

1.1.1 General

This document contains the specification for the user-network interface between the Nortel Networks IP Gateway(NT7X07AA) and terminal endpoints (terminals) designed for the Centrex IP Services of the DMS-100. The interfaces described in this document are based on the ITU-T H Series Recommendations, ISDN Q Series Recommendations, ISDN Standards established by ANSI/ECSA-T1, and the *ISDN Basic Interface Call Control Switching and Signaling Requirements* (TR-TSY-000268 Issue 3) and supplementary service Technical References and Generic Requirement documents published by Bellcore.

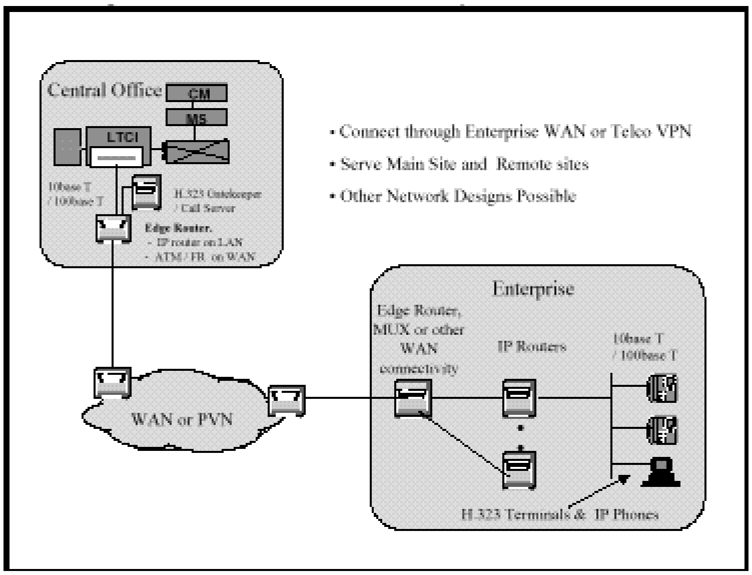
This release provides a comprehensive level of compliance to ITU-T recommendations H.323 and H.225.0, and describes Nortel Networks's offering of Centrex IP Services. Elements of the Bellcore variant of the Q.931 protocol used include the User-to-User Information Elements (UUIE) with the fastStart and the fastCap parameters and will be described in order to deliver the fast connect procedure.

1.1.2 Scope and objective

This document defines the characteristics of the interfaces between IP terminals and the IP Gateway terminating on a DMS-100 switch, the signaling procedures across the interfaces, and the capabilities provided by the DMS-100 switch to support the terminal.

It specifies how the terminals can gain access to the services and features provided by the DMS-100 IP Gateway. It also describes the facilities available in the DMS-100 switch to support terminals, and suggests ways in which terminal manufacturers can exploit these facilities to complement the network-provided services.

Figure 1 VOIP Connections to an Enterprise


Central Office
CM
MS
LTCI
10base T / 100base T
H.323 Gatekeeper / Call Server
Edge Router.
- IP router on LAN
- ATM / FR on WAN
• Connect through Enterprise WAN or Telco VPN
• Serve Main Site and Remote sites
• Other Network Designs Possible
WAN or PVN
Enterprise
Edge Router, MUX or other WAN connectivity
IP Routers
10base T / 100base T
H.323 Terminals & IP Phones

The remainder of Chapter 1 gives a brief description of the Centrex IP Services on DMS-100, terminal support philosophy and how Nortel Networks supports this philosophy in the DMS-100 switch.

1.1.3 Conformance

IP terminals claiming conformance to this specification are expected to conform to the following sections:

- Chapter 2, Physical Layer requirements, as appropriate
- Chapter 3, Data Link Layer requirements, as appropriate
- Chapter 4, Network Layer requirements, as appropriate
- Chapter 5, Transport Layer requirements, as appropriate
- Chapter 6, Call Signaling requirements that are applicable to terminals

1.2 Centrex IP Services Overview

The Centrex IP Services (ITS) primary function is to provide an interface between the infrastructure of the LAN world with the feature rich fabric of the PSTN. To provide this LAN-PSTN “bridging” functionality the ITS must support a myriad of traditional voice based services as well as LAN oriented protocols and services. In addition it must manage the necessary control and signaling protocols required to communicate with other H.323 elements. The various protocols specified by the H.323 Recommendation are shown in the following table.

Table 1: LAN based Multimedia Protocol Stack

<table>
<tr><th colspan="7">H.323/H.225.0 Protocol Stack</th></tr>
<tr><td>Audio Applications</td><td>Video Applications</td><td colspan="4">Terminal Control and Management</td><td>Data Applications</td></tr>
<tr><td>G.711
G.723.1</td><td>H.261
H.263</td><td rowspan="2">RTCP</td><td rowspan="2">H.225.0
RAS Channel</td><td rowspan="2">H.225.0
Call Signaling Channel</td><td rowspan="2">H.245
Call Control Channel</td><td>T.124</td></tr>
<tr><td colspan="2">RTP</td><td>T.125</td></tr>
<tr><td colspan="4">Unreliable Transport (UDP)</td><td colspan="2">Reliable Transport (TCP)</td><td rowspan="3">T.123</td></tr>
<tr><td colspan="6">Network Layer (IPv4)</td></tr>
<tr><td colspan="6">Data Link Layer (IEEE 802.3)</td></tr>
<tr><td colspan="7">Physical layer (IEEE 802.3)</td></tr>
</table>

1.2.1 Clarification of the ITU-T H.323 Protocols

In the NA012 release, only a subset of the H.323 protocol stack will be supported on the H.323 components (entities) as follows:

1.2.1.1 Protocols that will be supported

- H.225.00 RAS Channel Signaling
- Only the User-to-User Information Elements (UUIE) with the fastStart and the fastCap parameters in H.225.00 Call Signalling.
- TCP
- RTP/RTCP
- UDP
- IPv4
- Audio Codecs (G.711, and G.723.1)

For the NA012 release, the Bellcore variant of the Q.931 protocol as defined in NIS-S208-6, ISDN Basic Rate User Network Interface Specification, Issue 03.01, September, 1997, will be supported in order to deliver the existing National ISDN-2 (NI-2) feature set to market.

In NA012 the H.323 Gateway will only support H.323 speech calls. To provide PSTN switch service to H.323 terminals all speech calls will be routed via the Gateway. The Gateway, however, will disallow direct endpoint call signaling from the H.323 terminal.

1.2.1.2 Protocols Not Currently Supported

- Video Codecs (H.261, H.263)
- Data Channel (T.123, T.124, T.125)

1.3 Scope Limitations

The NA012 release will not support all items in the H.323 Recommendation. In particular, the following items are not supported in NA012:

- The Gateway is limited to support PSTN-H.323 speech calls, therefore neither video or data calls are supported.Specifically, the following items will not be supported in NA012:
  - — Video Codecs (H.261, H.263)
  - — Data Channel (T.123, T.124, T.125)
- Audio Codec (except G.711, and G.723.1,which will be supported in NA012).
- Full Gateway function (only a subset will be supported)
- Multipoint controller
- Multipoint processor
- Multipoint control unit
- H.323 Multipoint capabilities
- Full call signaling function. In particular, the following are not supported:
  - – Direct endpoint call signaling
  - – Direct H.245 control channel connection between endpoints
  - – Gatekeeper routed H.245 control

Chapter 2: Physical Layer Interface

2.1 Introduction

This Specification defines the Physical Layer (Layer 1) characteristics of the Centrex IP Services user-network interface supported on the DMS-100 switch. Two Layer 1 interfaces are defined:

- The Telephony/WAN Interface provides two full featured E1 (30 channel) or DS1(24 channel) interfaces. Alternatively, they can be configured as two unchanneled WAN interfaces running at 1.544/2.048 Mbps supporting either ISDN PRI or ATM data. While this interface exists, it is not intended to be the primary interface.
- A High Speed Datacom Interface provides three independent LAN interfaces, specifically, dual redundant 10/100 Mbps ISO/IEC 8802-3 (IEEE 802.3) compliant Ethernet interfaces and a 25.6 Mbps ATM25 interface. All three interfaces support Category 5 Unshielded Twisted Pair (UTP) cable directly. The ISO/IEC 8802-3 (IEEE 802.3) 10Base-T interface is the primary interface for the Centrex IP Services of the DMS-100.

2.2 Telephony/WAN Interface

2.2.1 E1 Interface

The 2048 Kbps, 30 channel primary multiplex system known as E1 is the most common system in use outside of North America. It was developed by the CEPT Administration and has been standardized by the CCITT/ITU where it is adequately described in Recommendations G.703 and G.732. Please refer to those documents if you require further details.

2.2.2 DS1 Interface

The 1544 Kbps, 24 channel DS1 or T1 primary multiplex system is a well known standard of the American National Standards Institute (ANSI) and will not be restated in this document. Please refer to the appropriate ANSI documentation if you require further details.

2.2.3 WAN Interface

This interface provides two unchannelized WAN links running at T1 or E1 speeds supporting ISDN PRI or ATM data. This configuration may be useful as a cost reduction for remote Gateway installations where external WAN routing equipment can be eliminated by connecting the WAN facilities directly to the Gateway card.

2.3 High Speed Datacom Interface

2.3.1 ISO/IEC 8802-3 (IEEE 802.3) Interface

Redundant 10/100 Mbps twisted pair ethernet interfaces are provided for LAN connectivity to CAT5 UTP cable via a 1:1 isolation transfomer.This connection provides full or half duplex connection to 10Base-T, or 100BaseT networks that are fully compliant with IEEE Std. 802.3. A 100Base-TX interface can also be configured that is fully compliant with the ANSI twisted-pair physical-media-dependent (TP-PMD) standard as well as IEEE Std. 802.3. The 10Base-T interface is intended to be the primary interface to the Centrex IP Services of the DMS-100

2.3.2 ATM25 Interface

The ITU-T ATM25 Interface provides the Transmission Convergence (TC) and Physical Media Dependent (PMD) layers of a 25.6 Mbps ATM interface suitable of ATM networks using Unshielded Twisted Pair (UTP) Category 3 (or better) wiring. This interface also provides an industry standard Universal Test and Operations PHY Interface for ATM (UTOPIA) interface for standardized control and communications to other components, such as Segmentation and Reassembly (SAR) controllers and ATM switches.

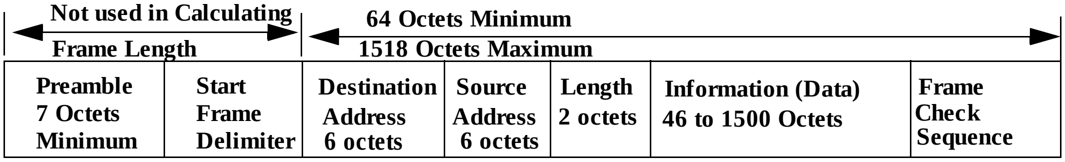
Chapter 3: Data Link Layer Interface

3.1 Introduction

3.1.1 General

ISO 8802-3 / IEEE 802.3 (Ethernet) is a packet based protocol standard for Local Area Networks employing Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method.

Figure 3-1 IEEE 802.3 Frame Structure



Preamble 7 Octets Minimum	Start Frame Delimiter	Destination Address 6 octets	Source Address 6 octets	Length 2 octets	Information (Data) 46 to 1500 Octets	Frame Check Sequence

Chapter 4: Network (IP)Layer

4.1 Introduction

4.1.1 General

The Centrex IP Services of the DMS-100 will support Internet Protocol Version 4 (IPv4 as defined by RFC 791) over a 10Base-T (Ethernet) loop (defined in ISO 8802-3 / IEEE 802.3). Protocols supported over this loop include the Internet Control Message Protocol (ICMP), Dynamic Host Configuration Protocol (DHCP), and User Datagram Protocol(UDP).

The format of a generic IP datagram is shown in Figure 4, IP Datagram

Figure 4 IP Datagram Format

0	4	8	16	19	24	31
VERS	HLEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS					PADDING	
DATA						
. . .						

Format.

The four bit VERS field defines the version of the IP protocol being used. It is currently set to 4 (0100). Datagrams with an unrecognized version will be rejected.

The Header Length (HLEN) field is also four bits long and specifies the length of the IP header. In the absence of IP OPTIONS this field is normally set to 20 octets long, which gives the field a minimum value of 5 (0101).

The SERVICE TYPE field sets the Quality of Service level. RFC 791 defines the eight bits of this field as defined in Figure 5, SERVICE TYPE Bit Definition.

Figure 5 SERVICE TYPE Bit Definition

0	1	2	3	4	5	6	7
Precedence			**D**	**T**	**R**	**Res (0)**	**Res (0)**

The Precedence bits specify the priority of the datagram, from 0 being used for routine datagram delivery to 7 being used for network control.

The D, T, and R bits specify the Delay, Throughput, and Reliability, respectively. The table below specifies the exact meaning of the bits.

Table 1 RFC 791 DTR Bit Definitions

D	T	R	Meaning
0			Normal Delay
1			Low Delay
	0		Normal Throughput
	1		High Throughput
		0	Normal Reliability
		1	High Reliability

Bit 6 has been proposed in RFC 1349 to mean “Minimize Monetary Cost”. As this RFC is not yet standard this bit will remain set to 0.

Bit 7 is reserved and is set to 0.

The TOTAL LENGTH field describes the length of the datagram (including both header and data) in octets. All hosts must accept datagrams up to 576 octets while always transmitting datagrams that exceed 576 octets

The IDENTIFICATION field identifies the datagram with a unique 16 bit number in case fragmentation becomes necessary.

The FLAGS field defines three flags used in processing fragments, if any. the first bit is reserved and is set to 0. The second bit controls whether or not fragmentation is allowed, and the third bit is sent when more fragments are to follow the current fragment.

The FRAGMENT OFFSET field defines the relative position of the fragment within the datagram structure.Measurement is done in 8 octet Fragment Blocks.

The TIME TO LIVE field defines the maximum time, in seconds, that the datagram may live on the internet. It is decremented by at least one at every hop (e.g. router) on its way to its destination. When the timer expires the datagram is discarded.

The PROTOCOL field identifies the next higher level protocol contained in the data area of the datagram. A list of well known protocols and their identification numbers is contained in RFC 1700.

The HEADER CHECKSUM field is an integrity check on the datagram header. It must be recalculated at every hop after the TIME TO LIVE field is modified.

The SOURCE IP and DESTINATION IP ADRESS fields have self evident definitions for specifying the transmitting host and final destination host.

The IP OPTIONS field consists of an 8 bit Option Type Octet defined in Figure 6, Option Type Octet Definitions below, an 8 bit Option Length octet (including Option Type, Length, and Data bits), and an Option Data octet.

Figure 6 Option Type Octet Definitions

Option Class	Option Number	Option Length	Option Name
0	0	-	End of Option List
0	1	-	No Operation
0	2	11	Security
0	3	Variable	Loose Source Routing
2	4	Variable	Internet Timestamp (round trip delay)
0	7	Variable	Route Record (source to destination)
0	8	4	Stream ID- obsolete
0	9	Variable	Strict Source Routing

The PADDING field ensures that the header ends on a 32 bit boundary.

Chapter 5: Transport Layer

5.1 Introduction

5.1.1 General

The Transport Layer uses the User Datagram Protocol (UDP), as described in RFC 768, to provide connectionless, best effort transmission of encoded voice datagrams/packets.UDP assumes the underlying protocol is IP but relies on a Reliability layer above UDP to provide more reliability than what is provided by IP. UDP is in effect a queue, distributing datagrams to the desired port identified in the received datagram.

The Transport Layer also uses the Transmission Control Protocol (TCP), defined in RFC 793 (updates in RFC's 1122, 813, 816, 879, and 896) to provide a reliable delivery service for call signaling. TCP assumes very little about the underlying protocol, but is used so frequently in conjunction with IP that the service it provides is best known as TCP/IP. Unlike UDP, TCP includes substantial functionality to ensure the reliability of the data stream.

5.2 Unreliable Transport (UDP)

A UDP packet is encapsulated within the data area of an IP packet, which is itself encapsulated within the Information field of an Ethernet frame as shown in Figure 5-1, “UDP Encapsulation”. The UDP Header is depicted in Figure 5-2, “UDP Header Format”.

Figure 5-1 UDP Encapsulation

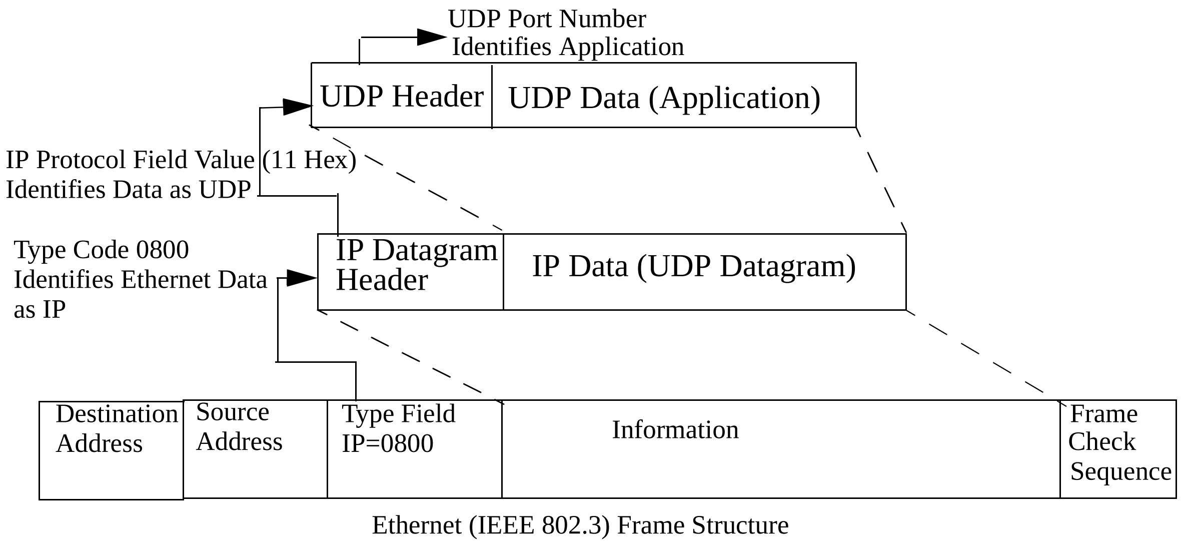


Figure 5-2 UDP Header Format

0 4 8 12 16 20 24 28 31

Source Port	Destination Port
Length	Checksum
Data	

The Source Port field is optional. When used, it is the port to which all replies should be sent. Well Known Ports are defined in Table 5-1, “Well Known UDP Port Numbers”

Table 5-1 Well Known UDP Port Numbers

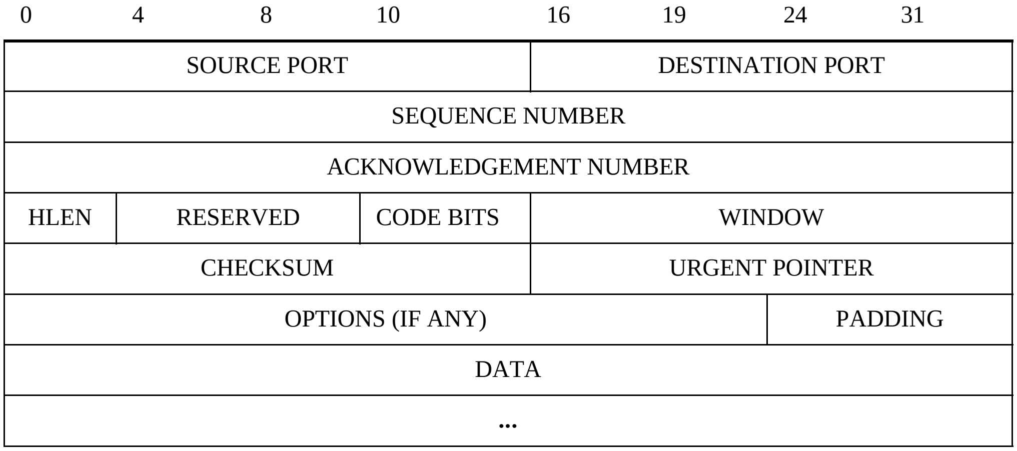
Port Number Decimal	Port No. Hex	Keyword	Description
7	0007	echo	Echo Protocol
9	0009	discard	Discard Protocol
11	000B	systat	Active Users Protocol
13	000C	daytime	Daytime Protocol
17	0011	qotd	Quote of the Day Protocol
19	0013	chargen	Character Generator Protocol
37	0025	time	Network Time Protocol
42	002A	nameserver	Host Name Server Protocol
43	002B	nicname	Who Is Protocol
53	0035	domain	Domain Name Server
67	0043	bootps	Boostrap Protocol (Server process)
68	0044	bootpc	Bootstrap Protocol (Client Process)
69	0045	tftp	Trivial File Transfer Protocol
161	00A1	snmp	Simple Network Management Protocol
162	00A2	Snmptrap	Simple Network Management Protocol Trap

5.3 Transmission Control Protocol (TCP)

Call signaling, which must be reliably transmitted, uses the Transmission Control Protocol (RFC 793) instead of the best effort UDP. Reliable transport of call signaling packets is dependent on the retransmission, end to end flow control, and network congestion controls of TCP. Among other functions TCP defines the format of data, the acknowledgment messages and procedures necessary to ensure reliable transmission of packets between systems. TCP can also distinguish between multiple destinations and can negotiate between systems prior to stream transfer. Multiple destinations are defined through the use of protocol port numbers which, like UDP, identify the destination of the packet. Unlike the queue like ports of UDP, TCP ports identify a virtual circuit between a pair of endpoints, also known as a socket. An endpoint is defined as a pair of integers which define the IP address for a host, and the TCP port on that host. A given TCP port can be shared by multiple connections on the same machine because TCP identifies its connections by pairs of endpoints(sockets).This allows for concurrent service to multiple connections simultaneously without the need for local port numbers for each connection.

5.3.1 TCP Segment Format

Figure 5.7 TCP Segment Header



0 4 8 10 16 19 24 31

SOURCE PORT			DESTINATION PORT	
SEQUENCE NUMBER				
ACKNOWLEDGEMENT NUMBER				
HLEN	RESERVED	CODE BITS	WINDOW	
CHECKSUM			URGENT POINTER	
OPTIONS (IF ANY)				PADDING
DATA				
...				

SOURCE PORT/DESTINATION PORT - Contains the TCP port numbers that identify the applications at the ends of the socket.

SEQUENCE NUMBER - The packet's position in the sender's data stream.

ACKNOWLEDGEMENT NUMBER - The number of the octet that the sender expects to receive next. If the applications send data simultaneously, a situation could arise where the acknowledgment from sender to receiver is sent in the same segment as data traveling from sender to receiver, but refers to data sent from receiver to sender. This is called piggybacking and is rarely used since most applications don't transmit simultaneously.

HLEN - Contains the offset of the data area within the segment, measured in multiples of 32 bits.This is necessary because the OPTIONS field is of variable length.

RESERVED - self explanatory.

CODE BITS - 6 bits which specify the purpose and contents of the segment as defined below.

Figure 5.8 Code Bits

Bit (left to right)	Meaning if bit set to 1
URG	Urgent Pointer field is valid
ACK	Acknowledgment field is valid
PSH	This segment requests a push
RST	Reset the connection
SYN	Synchronize sequence numbers
FIN	Sender has reached the end of its data stream

WINDOW - For the purposes of Flow Control, TCP advertises how much data it is willing to accept by specifying its buffer size in the WINDOW field.

CHECKSUM - A 16 bit integer checksum used to verify the integrity of the data, including the TCP Header.

URGENT POINTER - When the URG Code Bit is set the URGENT POINTER specifies the position of the end of urgent data within the segment.

OPTIONS (IF ANY) - Varies in length in multiples of 8 bits. Currently defined options include (kind indicated in octal):

Kind	Length	Meaning
0	-	End of Option List
1	-	No-Operation
2	4	Maximum Segment Size

End of Option List (00000000) -This option indicates the end of the option list. Usually only used if the end of the options don’t coincide with the end of the TCP header. There is no guarantee that senders will use this option, so receivers must process options even if they don’t begin on begin on a word (16 bit) boundary

No-Operation (00000001) - This option code can be used between options, to align the beginning of a subsequent option on a word boundary. There is no guarantee that senders will use this option, so receivers must process options even if they do not begin on a word boundary.

Maximum Segment Size (00000010 00000100 max seg size) - Possibly the most frequently used option, set by the receiver at the initial connection request to define the maximum buffer size the receiver can handle. If this option is not used, any segment size is allowed.

PADDING - Variable length (all zeros) used to ensure the TCP header ends on a 32 bit boundary.

5.3.2 Socket Initialization

TCP is a connection oriented protocol which requires both endpoints of a connection to agree that a connection is desired. The application layers of both endpoints start in a passive open state and wait for an incoming connection. The initiating endpoint (A) must perform an active open request to establish the connection. It does this by passing its initial sequence number (x) in a TCP header segment with the CODE BITS set to SYN. The receiving machine (B) records the sequence number of the transmitter (A) and replies by sending its initial sequence number (y) together with an acknowledgment that the receiver(B) expects to get sequence x+1 in the next transmission. The transmitter (A) then acknowledges receiving all octets through y from B.The socket is now initialized and ready to pass data. At this point all future acknowledgments in this session use the number of the next octet expected.

5.3.3 Sliding Windows and Flow Control

The first step in flow control is in getting the two TCP application layers to agree on a maximum segment size (OPTIONS Kind 2) to be used during the current session. The Maximum Segment Size (MSS) used in a session is defined by the receiver since the transmitter may not necessarily know the receivers buffer size. The receiver sends its MSS to the transmitter through the OPTIONS bits (Options Kind 2) of the TCP header. The transmitter receives the MSS and sets its transmission segment size accordingly. As the receiver’s buffer size changes, the WINDOW field of the TCP header is used to dynamically advertise the current receiver buffer size. Flow control is achieved by reducing the advertised WINDOW size from the MSS to zero to stop all transmission while the network recovers.

A Sliding Window is used to make full duplex transmissions more efficient as simplex transmissions can waste considerable bandwidth due to machine delayed responses. A Sliding Windows protocol allows multiple packets to be transmitted before waiting for an acknowledgment.

5.3.4 Timeouts and Retransmission

A reliable data stream requires the destination to send an acknowledgment of any segments sent. If the acknowledgment does not arrive within the expected time window, the transmitter assumes that its segment was lost or corrupted and retransmits it. Every time a segment is sent, a timer is started, based upon the average round trip delay measured during initialization of the socket. As each new segment is sent, TCP records the time, and the time the acknowledgment for that segment arrives. The Round Trip Time (RTT) is then adjusted based on the latest measure of network conditions. In the event packets are lost due to some network impediment, TCP increments the timeout using the delay along any path in the network on every transmission as a maximum limit. When acknowledgments start arriving in less delay times, the RTT is recalculated.

5.3.5 Congestion & Recovery

Congestion happens and routers have finite buffers, so in addition to storing the receiver's advertised buffer size (WINDOW in an acknowledgment segment), TCP also maintains a second limit called the congestion window. At any one time TCP will consider the actual WINDOW to be the minimum of the advertised window, and the congestion window. In the event of segment loss, the congestion window is reduced by half to a minimum of one segment. If segment loss continues once the minimum is reached TCP continues to double timeout values before retransmitting.

When congestion ends, a slow start recovery is used where the congestion window is increased by one every time an acknowledgment is received.

5.3.6 Closing a Socket

When an application concludes sending data it sends a segment with the FIN bit set (least significant CODE BIT). The receiver acknowledges the FIN segment, but waits until the receiving application is finished transmitting before sending its own FIN segment.It also ignores further transmission other than acknowledgments to what it sends. When the receiver is finally finished it sends the transmitter a FIN segment, which the transmitter acknowledges. When the final acknowledgment is received by the Receiver, the socket is erased by both endpoints.

5.3.7 Well Known Port Numbers

Like UDP, TCP has a set of well known port numbers for standard applications. Originally port numbers less than 256 were reserved for system use, but recently numbers up to 1024 have been assigned. Figure 5.9, "Well Known TCP Port Numbers", lists currently assigned port numbers.

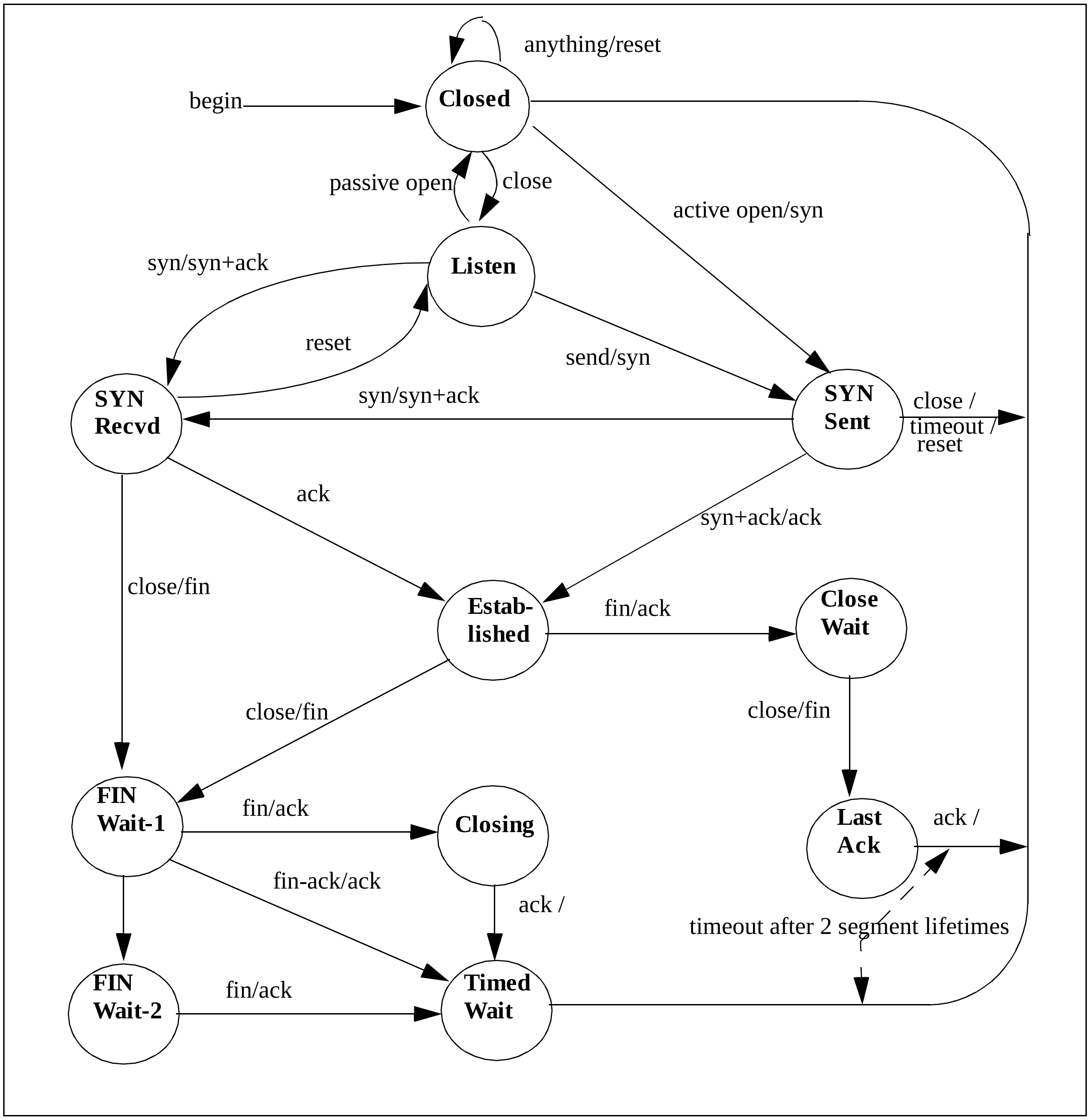
Figure 5.9 Well Known TCP Port Numbers

Decimal	Keyword	Description
0	-	Reserved
1	TCPMUX	TCP Multiplexer
5	RJE	Remote Job Entry
7	ECHO	Echo
9	DISCARD	Discard
11	USERS	Active Users
13	DAYTIME	Time of Day
15	-	Network Status Program
17	QUOTE	Quote of the Day
19	CHARGEN	Character Generator
20	FTP-DATA	File Transfer Protocol Data
21	FTP	File Transfer Protocol
23	TELNET	Terminal Connection
25	SMTP	Simple Mail Transport Protocol
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
77	-	Any Private RJE service
79	FINGER	Finger
93	DCP	Device Control Protocol
95	SUPDUP	SUPDUP protocol
101	HOSTNAME	NIC Host Name Server
102	ISO-TSAP	ISO-TSAP
103	X400	X.400 Mail Service
104	X400-SND	X.400 Mail Sending
111	SUNRPC	SUN Remote Procedure Call
113	AUTH	Authentication Service
117	UUCP-PATH	UUCP Path Service
119	NNTP	USENET News Transfer Protocol
129	PWDGEN	Password Generator Protocol
139	NETBIOS-SSN	NETBIOS Session Service
160-223	Reserved	

5.3.8 TCP Finite State Machine

TCP can best be understood through a state machine diagram as show below. The circles represent states, with arrows representing the transitions between states. The labels on the transitions describe what caused the transition and what its response is.

Figure 5.10 TCP Finite State Machine



Chapter 6: Terminal Control & Management

6.1 Addresses

- IP address

In NA011, every H.323 terminal shall have one IP address. Every H.323 Gateway and Gatekeeper shall have at least one IP address.

- TSAP identifier

For every IP Address, each H.323 entity may have several TSAP identifiers.

- Alias address

Every H.323 terminal has one or more DNs as alias addresses.

6.2 Call Reference Value (CRV)

A call reference value will be used to associate all call signaling messages related to the same call between two H.323 entities, for example, endpoint to Gatekeeper.

6.3 Call Identifier (Call ID)

A call ID is a globally unique non-zero value created by the calling endpoint. A call ID is used to associate all messages including RAS and call signalling messages related to the same call among all H.323 entities.

The call ID is different from the CRV in that the CRV has local significance only (between two entities) while the call ID is used globally for all the entities within the same call.

6.4 H.225.0 RAS

The Registration, Admission, and Status (RAS) signaling function uses the ITU-T Recommendation H.225.0 messages below to perform discovery, registration, admissions, and disengagement procedures between endpoints and Gatekeepers.

6.4.1 Discovery Messages

6.4.1.1 GatekeeperRequest (GRQ)

Note that one GRQ is sent per logical endpoint; thus an MCU or a Gateway might send many.

The GRQ message includes the following:

requestSeqNum - this is a monotonically increasing number unique to the sender. It shall be returned by the receiver in any messages associated with this specific message.

protocolIdentifier - identifies the H.225.0 vintage of the sending endpoint.

nonStandardData - carries information not defined in this recommendation (for example, proprietary data)

rasAddress - this is the transport address that this endpoint uses for registration and status messages.

endpointType - this specifies the type(s) of the endpoint that is registering (the MC bit shall not be set by itself).

gatekeeperIdentifier - string to identify the gatekeeper from which the terminal would like to receive permission to register. A missing or null string gatekeeperIdentifier indicates that the terminal is interested in any available gatekeeper.

callServices - provides information on support of optional Q-series protocols to gatekeeper and called terminal.

endpointAlias - a list of alias addresses, by which other terminals may identify this terminal

alternateEndpoints - a sequence of prioritized endpoint alternatives for rasAddress, endpointType, or endpointAlias

tokens - This is some data which may be required to allow the operation. The data shall be inserted into the message if available.

cryptoTokens - encrypted tokens

authenticationCapability - This indicates the authentication mechanisms supported by the endpoint.

algorithmOIDs -

integrity - indicates to the recipient which integrity mechanism is to be applied on the RAS messages

integrityCheckValue - provides improved message integrity/message authentication of the RAS messages. The cryptographically based integrity check value is computed by the sender applying a negotiated integrity algorithm and the secret key upon the entire message. Prior to integrityCheckValue computation this field shall be ignored and shall be empty. After computation, the sender puts the computed integrity check value in the integrityCheckValue field and transmits the message.

6.4.1.2 GatekeeperConfirm (GCF)

The GCF message includes the following:

requestSeqNum - This shall be the same value that was passed in the GRQ.

protocolIdentifier - identifies the vintage of the accepting gatekeeper.

nonStandardData - carries information not defined in this recommendation (for example, proprietary data)

gatekeeperIdentifier - string to identify gatekeeper that is sending the GCF.

rasAddress - this is the transport address that the gatekeeper uses for registration and status messages.

alternateGatekeeper - sequence of prioritized alternatives for gatekeeperIdentifer and rasAddress. The client should use these alternatives in the future should a request to the gatekeeper not respond or return a reject without redirect.

authenticationMode - This indicates the authentication mechanism to be used. The gatekeeper must choose authenticationMode from authenticationCapability provided by the endpoint in GRQ.

tokens - This is some data which may be required to allow the operation. The data shall be inserted into the message if available.

cryptoTokens - encrypted tokens

algorithmOID -

integrity - indicates to the recipient which integrity mechanism is to be applied on the RAS messages

integrityCheckValue - provides improved message integrity/message authentication of the RAS messages. The cryptographically based integrity check value is computed by the sender applying a negotiated integrity algorithm and the secret key upon the entire message. Prior to integrityCheckValue computation this field shall be ignored and shall be empty. After computation, the sender puts the computed integrity check value in the integrityCheckValue field and transmits the message.

6.4.1.3 GatekeeperReject (GRJ)

The GRJ message includes the following:

requestSeqNum - This shall be the same value that was passed in the GRQ.

protocolIdentifier - identifies the vintage of the rejecting gatekeeper.

nonStandardData - carries information not defined in this recommendation (for example, proprietary data)

gatekeeperIdentifier - string to identify gatekeeper that is sending the GRJ.

rejectReason - codes for why the GRQ was rejected by this gatekeeper.

alternateGatekeeper - sequence of prioritized alternateGatekeeper for gatekeeperIdentifer and rasAddress for client to retry the request

altGKisPermanent - TRUE if all future RAS signals should be redirected to an address from alternateGatekeeper, FALSE if only the message that caused the Reject should be redirected.

tokens - This is some data which may be required to allow the operation. The data shall be inserted into the message if available.

cryptoTokens - encrypted tokens

integrityCheckValue - provides improved message integrity/message authentication of the RAS messages. The cryptographically based integrity check value is computed by the sender applying a negotiated integrity algorithm and the secret key upon the entire message. Prior to integrityCheckValue computation this field shall be ignored and shall be empty. After computation, the sender puts the computed integrity check value in the integrityCheckValue field and transmits the message.

6.4.2 Registration Messages

6.4.2.1 RegistrationRequest (RRQ)

Supported as described in Recommendation H.225.0 Section 7.9.1

6.4.2.2 RegistrationConfirm (RCF)

Supported as described in Recommendation H.225.0 Section 7.9.2

6.4.2.3 RegistrationReject (RRJ)

Supported as described in Recommendation H.225.0 Section 7.9.3

6.4.3 Unregistration Messages

6.4.3.1 UnregistrationRequest (URQ)

Supported as described in Recommendation H.225.0 Section 7.10.1

6.4.3.2 UnregistrationConfirm (UCF)

Supported as described in Recommendation H.225.0 Section 7.10.2

6.4.3.3 UnregistrationReject (URJ)

Supported as described in Recommendation H.225.0 Section 7.10.3

6.4.4 Admission Messages

6.4.4.1 AdmissionRequest (ARQ)

Supported as described in Recommendation H.225.0 Section 7.11.1

6.4.4.2 AdmissionConfirm (ACF)

Supported as described in Recommendation H.225.0 Section 7.11.2

6.4.4.3 AdmissionReject (ARJ)

Supported as described in Recommendation H.225.0 Section 7.11.3

6.5 H.225.0 Call Signaling

As mentioned in section 1.2.1, "Clarification of the ITU-T H.323 Protocols", the Bellcore variant of the Q.931 protocol and the UUIEs (User-to-User Information Elements) with the fastStart and the fastCap parameters in H.225.0 call signalling are supported in the NA011 release.

All existing Q.931 information elements continue to be supported except the bearer capability information element which is restricted to the following code point:

- The *information transfer capability (octet 3)* must indicate either “speech” or “3.1-kHz audio”.
- The *information transfer rate (octet 4)* must indicate “64-kbps, circuit mode”.
- *Rate multiplier (octet 4.1)* shall not be used.
- The *User Information layer 1 protocol (octet 5)* must indicate “recommendation G.711 u-law”

6.5.1 H.323 User Information

The H.323 User Information structure contains two structures. These structures define the H.323 User-to-User Protocol Data Unit (H.323 UU PDU) and the User-Data.

The H.323 UU PDUs are mandatory. The User-Data is optional. User-Data is used to contain the information which would normally occupy the *User-user information* in a Q.931 message. The NA011 Centrex IP Services will not support User-Data.

.

```
H323-UserInformation:= SEQUENCE
{
        h323-uu-pdu H323-UU-PDU,
        user-data SEQUENCE
        {
                protocol-discriminator INTEGER (0.255),
                user-information OCTET STRING (SIZE(1.131)),
        } OPTIONAL,
                ...
}
```

user-data *is*
Not Supported

```
H323-UU-PDU:= SEQUENCE
{
        h323-message-body:= CHOICE
        {
                setup Setup-UUIE,
                callProceeding CallProceeding-UUIE
                connect Connect-UUIE,
                alerting Alerting-UUIE,
                releaseComplete ReleaseComplete-UUIE,
                progress Progress-UUIE,
                userInformation UI-UUIE
                facility Facility-UUIE,
                        ...
          }
          nonStandardData NonstandardParameter OPTIONAL,
                ...
  }
```

userInformation *and*
facility *are*
Not Supported

6.5.1.1 Support of UU PDUs

-> Alerting-UUIE

The NA011 Centrex IP Services will support all fields as defined in H.225.0.

-> CallProceeding-UUIE

The NA011 Centrex IP Services will support all fields as defined in H.225.0.

-> Connect-UUIE

The NA011 Centrex IP Services will support all fields as defined in H.225.0.

-> Setup-UUIE

The NA011 Centrex IP Services will support all fields as defined in H.225.0.

6.6 Call Signaling Procedures

According to Recommendation H.323, the provision of H.323 communications is divided into five phases. These are

- Phase A: Call set-up
- Phase B: Initial communication and capability exchange
- Phase C: Establishment of audio visual communications
- Phase D: Call Services
- Phase E: Call Termination

For the NA011 release, Call Services (Phase D) will not be supported. Call set-up, initial communication and capability exchange, and establishment of audio visual communications (Phase A, B, and C) will be combined and simplified using the fast connect procedure.

The fast connect procedure supports two parameters (fastCap and fastStart) that provide the audio mode information that would normally be passed later in the H.245 TerminalCapabilitySet and OpenLogicalChannel messages. The fastStart parameter must be used to support the signalling required to open a logical channel such as RTP/RTCP transport addresses and the fastCap parameter may be used to indicate the capabilities such as audio capability (g71lUlaw64k) that the H.323 terminal supports during the fast setup mode.

6.6.1 Use of Q.931

Q.931 is used throughout the call set-up phase (Setup, Call Proceeding, Alerting, Connect) and is used to close the Call Signaling Channel in the call termination phase (Disconnect, Release, Release Complete). In general, the symmetric procedures (i.e., class II procedures) are used. Most noticeably, these procedures allow only point-to-point transmission of the Setup message and mandates the use of network side timers T303, T301[1] on the user side.

Time s	Default Value	Cause for start	Normal Stop	At first expiry	At second expiry	Notes
T301	minimum 3 min	**Alerting** received	**Connect** received	Clear call	Timer is not restarted	The value of T301 is datafillable for the DMS.
T303	4 seconds	**Setup** sent	**Alert**, **Connect**, **Call Proc**, or **Rel Complete** received	Retransmit **Setup** and restart T303	Clear call	The BRI code currently supports the class 1 value of 2.5 seconds

6.6.2 Call set-up, initial communication and capability exchange, and establishment of audio visual communications

Prior to the call establishment, the endpoint terminal and the Gateway must have registered with the Gatekeeper and the Gatekeeper routed call signalling method has been chosen (i.e., the Gatekeeper will route the call signalling messages between the H.323 endpoints).

The endpoint terminal shall include the Calling Party Number (CPN) information element in the SETUP message sent to the Gatekeeper. The Gatekeeper shall authenticate the CPN information element and supply one if necessary.

To activate the fast connect procedure, the SETUP message from the calling endpoint must include the fastStart parameters in the User-to-User information element (UUIE). The called point must return a fastStart in the Call Proceeding, Alerting, or Connect messages. The called endpoint should return the RTP/RTCP Transport addresses that it wants the calling endpoint to use. The fastStart parameter contains sequence of the following fields:

- Open Logical Channel
  Only uni-directional procedures are supported since they are used for the transmission of audio traffic.

  + *forward Logical Channel Number*

    This is encoded as shown in H.245.

[1] Symmetric procedures mandate the use of T310 in certain cases, but T310 isn't required in H.225.0

+ forward Logical Channel Parameters

This contains the parameters associated with the logical channel. It is composed of the ASN.1 code points

portNumber - This code point is optional.

dataType - Should use the structure AudioData. AudioData should be encoded using the ASN.1 code point **g711Ulaw64k, g7231, or g729AnnexA**.

multiplexParameters - Should use **h225LogicalChannelParameters** structure. The **sessionID** field of **h225LogicalChannelParameters** should be set to 1 since 1 indicates the primary audio session established by fastStart.

+ reverse Logical Channel Parameters

This structure is used when opening a bi-directional logical channel.

The Setup message may also include the fastCap parameter to indicate a set of alternative capabilities the calling endpoint supports. The fastCap parameter contains the following two fields:

- MultiplexCap (Multiplex Capability)
  This is encoded using the ASN.1 structure **h2250Capability**. This contains various information regarding the transmission path and conferencing. It should encoded as follows

  maximumAudioDelayJiter - Set to any allowable value.

  receiveMultipointCapability, **transmitMultipointCapability, and receiveAndTransmitMultipointCapability -** All the ASN.1 code points in these structures should be set to false, except **Centralized Control** and **Audio** which should be set to true as mandated for H.323 terminals in H.245. Optional fields should not be present.

  mcCapability - Both the code point should be set to false.

  rtcpVideoControlCapability - Should be set to false.

  MediaPacketizationCapability - The fields present here should be set to false.

- Caps (Capabilities)
  Only the audio capability will be supported. The ASN.1 codepoint **capability** should be set to **receiveAudioCapability** and **transmitAudioCapability** and the ASN.1 codepoint **audioCapability** should be set to **g711Ulaw64k, g7231, or g729AnnexA**.

6.6.3 Call Termination

Call termination (a.k.a. call clearing) can be initiated from the PSTN terminal, from the endpoint terminal, or initiated simultaneously by sending a Q.931 Disconnect message on the Call Signaling Channel and the Call Signaling Channel is closed.

6.7 Protocol Requirements

As mentioned in previous sections, one of the objectives for the NA011 Centrex IP Services is to offer a set of NI-2 services over a packet based network.
This section describes the protocols required in order to support NI-2 services (which are available on the DMS) on top of a H.323 protocol stack.

6.7.1 Comparison of Protocol Definitions

6.7.1.1 Basic Call Signalling Difference

The protocol difference between ITU-T Q.931, Bellcore's variant of Q.931 as supported on the DMS, and ITU-T H.323 from the basic call perspective is examined. The differences in the following areas are highlighted:

- messages for circuit-switched connection control
- information elements (IEs)
- code points
- message details with mandatory or optional IEs

6.7.1.2 Supplementary Services and Extensions

The additional protocol requirements for supplementary services and extensions are also examined as follows:

- supplementary services such as Call Forwarding and Flexible Call using generic feature key management procedures - feature activation/feature indication (FA/FI) (including recommendations on assignment of Fixed Feature Identifiers) and Q.932 messages
- EKTS with network specific messages
- National Specific (codeset 5) IEs
  - — Display Text (DT)
  - — Operator System Assistance (OSA)
- Network Specific (codeset 6) IEs
  - — Call Appearance

6.7.2 High-Level Protocol Description

6.7.2.1 ITU-T Recommendation H.323 protocol stack

The H.323 protocol stack is defined in the following documents:

- Draft ITU-T Recommendation H.323V2 (1998): “Packet Based Multimedia Communications Systems”

- Draft ITU-T Recommendation H.225.0, Version 2 (March 25, 1997): “Call Signalling Protocols and Media Stream Packetization and Synchronization for Packet Based Multimedia Communications Systems”
- ITU-T Recommendation H.245 - Version 2 (December 13, 1996): “Control Protocol for Multimedia Communication”

See Figure 1, "LAN based Multimedia Protocol Stack," on page 11 for details.

Assumption: products that claim compliance with version 2 of H.323 must comply with all of the mandatory requirements of the H.323V2 (1998) document, including references to requirements captured in H.225.0 (1998) and H.245 (1998).

The protocol of interest that is used in the comparison below is H.225.0 Call Signalling. Other H.323 protocols such as H.225.0 RAS, RTP/RTCP, and H.245 Control shall also be supported. Note that the fast connect procedure shall be supported in NA011.

6.7.2.2 ITU-T Recommendation Q.931 (1993)

Q.931 requirements are defined in:

ITU-T Recommendation Q.931 (1993): “ISDN User-Network Interface Layer 3 Specification for Basic Call Control”

6.7.2.3 Bellcore protocols that are supported on the DMS (ISDN BRI)

DMS ISDN BRI protocol is defined in:

- Nortel NIS S208-6 version 03.03: “ISDN BRI Interface Specification” including
  - National Specific (codeset 5) IEs
    - Display Text (DT) - ANSI T1.610A (1990)
    - Operator System Assistance (OSA)
  - Network Specific (codeset 6) IEs
    - Call Appearance
- Bellcore’s variant of Q.931 as defined in TR-268, SR-3888
- Q.932 messages as captured in TR-861
- Bellcore GR-205, Issue 1, Revision 1: “ISDN EKTS Generic Requirements”, which captures EKTS specific messaging

6.7.3 Interoperability between H.225.0 and Q.931

As described in ITU-T H.225.0, Section 7.1, the H.225.0 endpoint may ignore all optional messages it does not support, but shall respond to an unknown message with a Status message. The endpoint shall be able to ignore unknown information elements.

6.7.4 Comparison of Protocols at Message level

The following notations used in Table 2, " Message Comparison” are adopted from ITU-T recommendation H.225.0:
where M = Mandatory, O = Optional, F = Forbidden, and CM = Conditional Mandatory. Additionally, ND is defined here for Not Defined, NS for Not Supported.

A message is considered “CM” if it shall be supported in some scenarios. For example, a terminal that uses Gateways is required to be able to receive and process the Call Proceeding message, but a terminal that does not use Gateways can optionally omit the message.

Comparison between ITU-T Q.931, Bellcore’s variant of Q.931, and H.225.0 is made using the above notations. Note that Bellcore’s variant of Q.931 BRI on the DMS is a user-to-network protocol versus H.225.0 which follows the symmetric call operation.

The “DMS Terminal Client” and the “DMS Gateway” columns indicate which messages are supported in the NA011 release.

Table 2 Message Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**		**ITU-T H.225.0 Call Signalling**		**DMS Terminal Client**		**DMS Gateway**	
	user-to-network	**network-to-user**	**Transmit (T)**	**Receive (R)**	**T**	**R**	**T**	**R**
Call establishment messages:								
Alerting	O	O	O[a]	CM[b]	Supported as defined in H.225.0			
Call proceeding	O	M	O	CM				
Connect	M	M	M	M				
Connect Acknowledge	O	M	F	F				
Progress	NS	O	O	O	Not supported			
Setup	M	M	M	M	Supported as defined in H.225.0			
Setup Acknowledge	NS	O	O	O				

Table 2 Message Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**		**ITU-T H.225.0 Call Signalling**		**DMS Terminal Client**		**DMS Gateway**	
	user-to-network	**network-to-user**	**Transmit (T)**	**Receive (R)**	**T**	**R**	**T**	**R**
Call Clearing messages:								
Disconnect	O	O	F	F	Supported as defined in H.225.0			
Release	O	O	F	F				
Release Complete	M	M	M[c]	M				
Call information phase messages:								
Resume	NS	NS	F	F	Supported as defined in H.225.0			
Resume Acknowledge	NS	NS	F	F				
Resume Reject	NS	NS	F	F				
Suspend	NS	NS	F	F				
Suspend Acknowledge	NS	NS	F	F				
Suspend Reject	NS	NS	F	F				
User Information	NS	NS	O	O	Not supported			
Miscellaneous Messages:								
Congestion Control	NS	NS	F	F	Supported as defined in H.225.0			
Information	O	O	O	O				
Notify	NS	O	O	O	NS	O	O	O
Status	O	O	M[d]	M	Supported as defined in H.225.0			
Status Enquiry	NS	O	O	M	NS	O	O	O
Q.932 Messages:								
Facility	Used only in Parameter Downloading		M	M	Supported as defined in H.225.0			

Table 2 Message Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**		**ITU-T H.225.0 Call Signalling**		**DMS Terminal Client**		**DMS Gateway**	
	user-to-network	**network-to-user**	**Transmit (T)**	**Receive (R)**	**T**	**R**	**T**	**R**
Hold	O	O	F	F	Supported as defined on the DMS			
Hold Acknowledge	O	O	F	F				
Hold Reject	O	O	F	F				
Retrieve	O	O	F	F				
Retrieve Acknowledge	O	O	F	F				
Retrieve Reject	O	O	F	F				
Network specific messages (for EKTS):								
Key Hold	NS	M	ND	ND	Supported as defined on the DMS			
Key Release	NS	M	ND	ND				
Key Setup	NS	M	ND	ND				
Key Setup Acknowledge	M	NS	ND	ND				
Parameter Downloading								
Facility	M	M	ND	ND	Not supported			
Register	M	M	ND	ND				
Segment	NS	O	ND	ND				

a. Note that this is different from the requirement stated in H.225.0/Table 4, which indicates the Alerting message is mandatory.

b. See a.

c. The Release Complete message is required for call clearing whenever the H.225.0 call signalling channel is open.

d. The Status message is required to respond to an unknown message. It is also required to respond to the Status Enquiry message with Status.

6.7.5 Comparison of Protocols at Information Element level

Table 2, " Message Comparison”, shows comparison for the three header information elements and other information elements. This table shows whether an information element is supported for each protocol. The detailed code points comparison is described in the next section.

Table 3 Information Element Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**	**ITU-T H.225.0**
Header information elements:		
Protocol Discriminator	08H	08H
Call Reference	CRV can be 1- 2 octets	CRV must be 2 octets
Message Type	Supported as defined in ITU-T Q.931 and TR-268 plus network specific message types.	Supported as defined in ITU-T Q.931 and H.225.0.
Single octet information elements:		
Locking shift	Supported as defined in TR-268.	Not defined
Non-locking shift	Not supported	Not defined
Congestion Level	Not supported	Shall not be used
More Data	Not supported	Shall not be used
Sending Complete	Not supported	Supported
Variable length information elements:		
Bearer Capability	Supported	Supported
Call Identity	Not supported	For future study
Call State	Supported	Supported
Called Party Number	Supported	Supported
Called Party Subaddress	Supported	Supported
Calling Party Number	Supported	Supported
Calling Party Subaddress	Supported	Supported
Cause	Supported	Supported
Channel Identification	Supported	For future study
Date/time	Not supported	Supported
Display	Not supported	Supported

Table 3 Information Element Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**	**ITU-T H.225.0**
High Layer Compatibility	Supported	For future study
Keypad Facility	Supported	Supported
Low Layer Compatibility	Supported	For future study
Network-specific Facilities	Not supported	Shall not be used
Notification Indicator	Supported	Supported
Progress Indicator	Supported	Supported
Repeat Indicator	Not Supported	Shall not be used
Restart Indicator	Not Supported	Shall not be used
Redirecting Number	Supported	Not defined
Segmented Message	Supported	Shall not be used
Signal	Supported	Supported
Transit Network Selection (TNS)	Supported	Shall not be used
User-user	Not Supported	Supported (see Section 6.5.1.1)
ITU-T Q.932 information elements:		
Endpoint Identifier (EID)	Supported	Not defined
Extended Facility	Used in Parameter Downloading only	Supported[a]
Facility	Used in NI-1 only	Supported[b]
Feature Activation	Supported	Not defined
Feature Indication	Supported	Not defined
Information Request	Supported	Not defined
Service Profile Identification (SPID)	Supported	Not defined
National specific information elements (codeset 5)		
Display Text (DT)	Supported	Not defined
Operator System Access(OSA)	Supported	Not defined
Network specific information elements (codeset 6)		
Call Appearance	Supported	Not defined

Table 3 Information Element Comparison

ITU-T Q.931	**Bellcore variant of Q.931 on the DMS (ISDN BRI)**	**ITU-T H.225.0**
Information elements for Parameter Downloading		
Extended Facility	Supported	Not supported
Segmented Message	Supported	Not supported

a. Either the Facility or the Extended Facility IEs is required if the Facility message is carrying Q.95x supplementary service signalling. Otherwise, the zero-length Facility IE may be required.

b. see a.

6.7.6 Comparison of Protocols at Code Point level

The following sections compare code points as supported on the DMS (ISDN BRI) versus the ones as defined in ITU-T H.225.0. Note that the comparison is made only for those information elements supported by both protocols. See NIS S208-6 version 03.03 for details on the information elements that are supported on the DMS.

6.7.6.1 Bearer Capability (BC)

Note that the only information transfer capability set by the H.323 endpoints shall be either “speech” or “3.1-kHz audio” since only speech calls are supported.

- The BC IE supported on the DMS (ISDN BRI) is shown in the following table:

Table 4 Bearer Capability

Encoding								**Attributes**	**Octet #**
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
(**1**) Speech, Circuit-mode (Octet 5a, 6 and 7 are not present)									
1	0	0	0	0	0	0	0	Transfer capability = speech	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit-mode 64 kb/s	4
1	0	1	0	0	0	1	0	Layer 1 protocol ID = Recommendation G.711 Mu-law	5
(**2**) 3.1 kHz, circuit-mode (Octet 5a, 6 and 7 are not present)									
1	0	0	0	1	0	0	0	Transfer capability = 3.1 kHz	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit, 64 kb/s	4
1	0	1	0	0	0	1	0	Layer 1 protocol ID = Recommendation G.711 Mu-law	5
(**3**) 64 kb/s, unrestricted digital information, rate adapted from 56 kb/s (Octets 6 and 7 are not present)									
1	0	0	0	1	0	0	0	Transfer capability = unrestr. digital	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit-mode 64 kb/s	4
0	0	1	0	0	0	0	1	Layer 1 protocol ID = Rate adaption	5
1	0	0	0	1	1	1	1	Data rate = 56 kb/s	5a
(**4**) 64 kb/s, unrestricted digital information, circuit-mode (Octets 5, 5a, 6, and 7 are not present)									
1	0	0	0	1	0	0	0	Transfer capability = unrestricted digital	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit-mode	4
(**5**) 64 kb/s restricted, circuit-mode (64 kb/s restricted, circuit-mode information may not be implemented on some networks; Octets 5, 5a, 6, and 7 are not present)									
1	0	0	0	1	0	0	1	Transfer capability = restricted digital	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit, 64 k/pd	4
(**6**) 7 kHz audio, circuit mode (Octet 5a, 6, and 7 are not present)									
1	0	0	1	0	0	0	1	Transfer capability = 7 kHz	3
1	0	0	1	0	0	0	0	Transfer mode and rate = circuit, 64 kb/s	4

Table 4 Bearer Capability

Encoding								Attributes	Octet #
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
1	0	1	0	0	1	0	1	Layer 1 protocol ID = Recomm. G.722/G.725	5

- The H.225.0 BC IE as defined in section 7.2.2.1/ITU-T H.225.0:
  - — The *information transfer capability (octet 3)* must indicate either “speech” or “3.1-kHz audio”.
  - — The *information transfer rate (octet 4)* must indicate “64-kbps, circuit mode”.
  - — *Rate multiplier (octet 4.1)* shall not be used.
  - — The *User Information layer 1 protocol (octet 5)* must indicate “recommendation G.711 u-law”

6.7.6.2 Call State

Note that call state values, 15 (Suspend request), 17 (Resume request), and 25 (Overlap receiving) as defined in ITU-T Q.931 are not supported on the DMS.

- The Call State values supported on the DMS (ISDN BRI) are shown in the following table:

Table 5 Call State information element

State No.	User State	Network State
0	Null	Null
1	Call Initiated	Call Initiated
2	Overlap Sending	Overlap Sending
3	Outgoing Call Proceeding	Outgoing Call Proceeding
4	Call Delivered	Call Delivered
6	Call Present	Call Present
7	Call Received	Call Received
8	Connect Request	Connect Request
9	Incoming Call Proceeding	Incoming Call Proceeding
10	Active	Active
11	Disconnect Request	Disconnect Request
12	Disconnect Indication	Disconnect Indication
19	Release Request	Release Request
22	N/A	Call Abort
31	Call Independent	Call Independent

- The Call State values defined in section 7.2.2.3/ITU-T H.225.0 are set per ITU-T Q.931 with some restrictions that need to be clarified.

6.7.6.3 Called Party Number (CDN)

Note that in ITU-T H.225.0, if the Numbering Plan Identification is set to Private Numbering Plan in a packet based network originated call, this indicates that the E.164 address is not present in the SETUP message and the call will be routed via an alias address in the UUIE.

- The CDN IE with its code points supported on the DMS (ISDN BRI) is shown in the following table:

Table 6 Called Party Number information element

8	7	6	5	4	3	2	1	**Octet**
0	Called Party Number information element Identifier							1
	1	1	1	0	0	0	0	
Length of called party number contents								2
1 EXT	Type of Number							3
	0	0	0	Unknown (note1)				
	0	0	1	International number				
	0	1	0	National number				
	0	1	1	Network specific number				
	1	0	0	Subscriber number				
	1	1	0	Abbreviated number				
				Al other values are reserved				
				Numbering Plan Identification				
	Unknown			0	0	0	0	
	Telephony/ISDN Numbering Plan (Rec. E.164			0	0	0	1	
	Data numbering plan (REC X.121) **+ (Note 3)**			0	0	1	1	
	Private numbering plan			1	0	0	1	
	Al other values are reserved							
0	Number Digits (IA5 characters)							4 * etc.

Note 1: The type of number "unknown" is frequently used when the network has no knowledge of the type of number in the number digits field. In this case, the number digits field is organized according to the network dial plan, for example, prefix or escape digits may be present.

Note 2: The number digit in octet 4 precedes the digit in octet 5, etc.The address digit which would be "dialed" first is located in octet 4.

Note 3: + = Packet mode calls are not currently supported

Note 4: Prefix and escape digits are not included for all values except “unknown”.

- The H.225.0 CDN IE is defined in section 7.2.2.4/ITU-T H.225.0.

6.7.6.4 Called Party Subaddress

Note that the Called Party Subaddress code points supported on the DMS (ISDN BRI) as shown below are the same as the ones defined in section 7.2.2.5/ITU-T H.225.0.

Table 7 Called Party Subaddress information element Identifier

8	7	6	5	4	3	2	1	**octet**
0	Called Party Subaddress Information element identifier							1
	1	1	1	0	0	0	1	
Length of called party subaddress information								2
1 Ext	Type of Subaddress			odd/ even indication	Spare			3
					0	0	0	
				0	even number of digits in subaddress			
				1	odd number of digits in subaddress			
	0	0	0	NSAP (X.213/ISO 8348 AD2)				
	0	1	0	user specified				
				All other values are reserved				
Subaddress Information								4 * etc.

6.7.6.5 Calling Party Number (CPN)

Note that in ITU-T H.225.0, if the Numbering Plan Identification is set to Private Numbering Plan in a packet based network originated call, this indicates that the E.164 address is not present in the SETUP message and the call will be routed via an alias address in the UUIE.

- The CPN IE with its code points supported on the DMS (ISDN BRI) is shown below:

Table 8 Calling Party Number Information Element Octet 3

7	**6**	**5**	**4**	**3**	**2**	**1**	**Meaning of Octet 3**
Type of Number			Number Plan Identification				
0	0	0					Unknown
0	0	1					International Number
0	1	0					Network Specific Number (Not currently supported)
1	0	0					Subscriber Number (Note 5)
1	1	0					abbreviated Number

7	**6**	**5**	**4**	**3**	**2**	**1**	**Meaning of Octet 3**
			4	**3**	**2**	**1**	Numbering Plan Identification
			0	0	0	0	Unknown
			0	0	0	1	Telephony/ISDN Numbering Plan (Rec. E.164)
			0	0	1	1	Data Numbering Plan (Rec. X.121) Not currently supported
			1	0	0	1	Private Numbering plan
							All other values reserved

Note 5: only supported in user to network direction

Note 6: Prefix and escape digits are not to be included in the “Number Digits” field.

- The H.225.0 CPE IE is defined in section 7.2.2.6/ITU-T H.225.0.

6.7.6.6 Calling Party Subaddress

Note that the Calling Party Subaddress code points supported on the DMS (ISDN BRI) as shown below are the same as the ones defined in section 7.2.2.7/ITU-T H.225.0.

Table 9 Calling Party Subaddress information element

8	7	6	5	4	3	2	1	**Octet**
0	Called Party Subaddress information element Identifier							1
	1	1	1	0	0	0	1	
Length of Called Party Subaddress information								2
1 Ext	Type of Subaddress			odd/ even indication	Spare			3
					0	0	0	
				0	even number of digits in subaddress			
				1	odd number of digits in subaddress			
	0	0	0	NSAP (X.213/ISO 8348 AD2)				
	0	1	0	user specified				
				All other values are reserved				
Subaddress Information								**4 * etc**.

6.7.6.7 Cause

- The Cause values supported on the DMS (ISDN BRI) are defined in section 4/NIS S208-6 version 03.03.
- The H.225.0 Cause IE is defined in section 7.2.2.8/ITU-T H.225.0 with the following conditions:
  - — The Gateway must map from a ReleaseCompleteReason to the Cause information element when it sends a Release Complete message from the packet based network side to the circuit switched network side. The

reverse mapping is not required since H.323 entities must decode the Cause information element.

6.7.6.8 Notification Indicator (NI)

The Notification Description Values supported on the DMS are completely different from the ones defined in ITU-T Q.931. ITU-T H.225.0 Notification Indicator IE follows the one defined in ITU-T Q.931.
For more information, see Section 45.5.3.8/NIS S208-6 version 03.03 for the DMS NI and Section 4.5.22/ITU-T Q.931 for the H.225.0 NI.

6.7.6.9 Progress Indicator (PI)

The major differences are as follows:

— for Location, only code points, 'user', 'private network serving the local user', and 'private network serving the remote user' are supported in H.225.0.

— for Progress description code points, the DMS supports 1, 2, 3, 8, and 10 while the H.225.0 supports 1, 2, 3, 4, 5, and 8 where 4 is 'Call has returned to ISDN' and 5 is 'Interworking has occurred and has resulted in a telecommunication service change'.

- The PI IE with code points its supported on the DMS (ISDN BRI) are shown in the tables below:

Table 10 Progress Indicator Information Element

Bits								**Meaning**	
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		**Octet**
0	Progress Indicator Information Element Identifier								1
	0	0	1	1	1	1	0		
Length of progress indicator contents									2

Bits								**Meaning**	
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		**Octet**
1	Coding Standard		Spare	General Location					3
Ext.	7	6	5	**4**	**3**	**2**	**1**		
	0	0						CCITT standard	
	0	1						Reserved	
	1	0						National standard	
	1	1						Network-Specific standard	
			5					Spare	
			0					Bit (this value always = 0)	
				4	**3**	**2**	**1**	General Location	
				0	0	0	0	User	
				0	0	0	1	Private network serving local user (Note 3)	
				0	0	1	0	Public network serving local user	
				0	0	1	1	transit network (Notes 1 and 3)	
				0	1	0	0	public network serving remote user (Note 3)	
				0	1	0	1	private network serving remote user (Note 3)	
				0	1	1	1	International network (Notes 2 and 3)	
				1	0	1	0	network beyond interworking point (Note 3)	
								All other values are reserved	
1 Ext.	Progress Description								4

Note 1: The “transit network” codepoint does not apply to the CCITT-standardized coding standard.
Note 2: The “international network” codepoint applies only to the Network-specific coding standard.
Note 3: These values may not be sent in all situations.

Table 11 Octet 4 Progress description

Bits							**Number**	**Octet 4**
7	**6**	**5**	**4**	**3**	**2**	**1**		**CCITT Standardized Values (Coding Standard = 00)**
0	0	0	0	0	0	1	1	Call is not end-to-end ISDN further call progress information may be available inband
0	0	0	0	0	1	0	2	Called equipment is non-ISDN
0	0	0	0	0	1	1	3	Calling equipment is non-ISDN
0	0	0	1	0	0	0	8	In-band information or appropriate pattern is now available
All other values are reserved								
National Standard (coding Standard = 10)								
7	6	5	4	3	2	1	10	Delay in response at called interface

Table 11 Octet 4 Progress description

Bits							Number	Octet 4
7	**6**	**5**	**4**	**3**	**2**	**1**		**CCITT Standardized Values (Coding Standard = 00)**
All other values are reserved								

- The H.225.0 PI IE is defined in section 7.2.2.21/ITU-T H.225.0.

6.7.6.10 Signal

The major difference between the Bellcore’s variant of Q.931 Signal IE as supported on the DMS and the ITU-T Q.931 Signal IE is that the DMS supports additional network-specific Signal values but does NOT support the following Signal values:

— Answer tone on

— Call waiting tone

— Off-hook warning tone

— Preemption tone on

— Alerting on - pattern 5

— Alerting on - pattern 7

Note that the H.225.0 Signal IE is set as per ITU-T Q.931.

- The Signal IE with its code points supported on the DMS (ISDN BRI) is defined in section 4/NIS S208-6 version 03.03.
- The H.225.0 Signal IE is defined in section 7.2.2.26/ITU-T H.225.0.

6.7.7 Comparison of Protocols at Message Details level

The following sections compare message details as supported on the DMS (ISDN BRI) versus the ones as defined in H.225.0. Note that the messages supported by both protocols as described in Table 2, " Message Comparison" are compared here.

The "Direction" column only applies to the DMS messages. The "Type" column indicates whether a message is "M" - Mandatory, "O" - Optional, or "FFS"- For Future Study. The lengths of the IEs specified in the H.225.0 messages refer to the ones originated by H.323 endpoints only.

6.7.7.1 Alerting

ALERTing may be sent by the called entity, to indicate the initiation of that called user alerting.

Table 12 DMS Alerting

Information Element	**Direction**	**Type**	**Length**
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	M	1
Channel Identification	u-to-n	O	3
Progress Indicator	n-to-u	O	4
Signal	n-to-u	M	3
Redirecting Number	n-to-u	O	4-16
Redirection Number	n-to-u	O	6-13
Locking Shift **(%[a])**	n-to-u	O	1
Display Text	n-to-u	O	4-*

[a] % denotes codeset change.

Table 13 H.225.0 Alerting

Information Element	**Type**	**Length**
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Bearer Capability	O	5-6
Extended Facility	O	8-*
Channel Identification	FFS	NA
Facility	O	8-*
Progress Indicator	O	2-4

Table 13 H.225.0 Alerting

Information Element	**Type**	**Length**
Notification Indicator	O	2-*
Display	O	2-82
Signal	O	2-3
HLC	FFS	NA
User-to-User	M	2-131

6.7.7.2 CALL PROCeeding

CALL PROCeeding may be sent by the called entity, to indicate that the requested call establishment has been initiated, and no more call establishment information will be accepted.

Table 14 DMS CALL PROCeeding

Information Element	Direct	Type	Length
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	M	1
Channel Identification	both	M[a]	3
Progress Indicator	n-to-u	O	4
Notification indicator	n-to-u	O	3
Information Request	n-to-u	O	3
Signal	n-to-u	O	3
Feature Indication	n-to-u	O	4-5
Called Party Number	n-to-u	O	4-27
Called Party Subaddress	n-to-u	O	4-23
Redirection Number	n-to-u	O	6-13
Locking Shift **(%)**	n-to-u	O	1
Display Text	n-to-u	O	4-*

[a] Channel Identification - if this is the first message in response to a SETUP, mandatory in the network-to-user direction, It is included in the user-to-network direction if this is the first response to the SETUP for a basic call.

Table 15 H.225.0 Call Processing

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Bearer Capability	O	5-6
Extended Facility	O	8-*
Channel Identification	FFS	NA
Facility	O	8-*
Progress Indicator	O	2-4
Notification Indicator	O	2-*

Table 15 H.225.0 Call Processing

Information Element	**Type**	**Length**
Display	O	2-82
HLC	FFS	NA
User-to-User	M	2-131

6.7.7.3 CONNect

CONNect shall be sent by the called entity to the calling entity to indicate call acceptance by the called entity.

Table 16 DMS CONNect

Information Element	Direct	Type	Length
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	M	1
Connected number	n-to-u	O	4-16
Channel Identification	u-to-n	O	3
Progress Indicator	n-to-u	O	4
Notification indicator	n-to-u	O	3
Signal	n-to-u	O	3
User-User (+)	both	O	3-131
Locking Shift (%)	n-to-u	O	1
Display Text	n-to-u	O	4-*

Table 17 H.225.0 CONNect

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Bearer Capability	O[a]	5-6
Extended Facility	O	8-*
Channel Identification	FFS	NA
Facility	O	8-*
Progress Indicator	O	2-4
Notification Indicator	O	2-*
Display	O	2-82
Date/Time	O	8
HLC	FFS	NA
LLC	FFS	NA
User-to-User	M	2-131

[a] BC is mandatory if Connect is sent between an H.323 entity and a Gateway.

6.7.7.4 PROGress

On the DMS, the network sends a PROGress to indicate the progress of a call, in the event of interworking or in relation with the provision of in-band information/patterns.

In H.225.0, this message may be sent by a Gateway to indicate the progress of a call, in the event of interworking with PSTN. This message may be sent by an endpoint (a Gateway or a terminal) before Connect, depending on supplementary service interaction.

Table 18 DMS PROGress

Information Element	**Direct**	**Type**	**Length**
Protocol Discriminator	n-to-u	M	1
Call Reference	n-to-u	M	2-3
Message Type	n-to-u	M	1
Cause	n-to-u	O	4-5
Progress Indicator	n-to-u	M	4
Notification Indicator	n-to-u	O	3
Signal	n-to-u	O	3
Display Text	n-to-u	O	4-*

Table 19 H.225.0 PROGress

Information Element	**Type**	**Length**
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Bearer Capability	O[a]	5-6
Cause	O	2-32
Extended Facility	O	8-*
Channel Identification	FFS	NA
Facility	O	8-*
Progress Indicator	O	2-4
Notification Indicator	O	2-*
Display	O	2-82
HLC	FFS	NA
User-to-User	M	2-131

[a] BC is mandatory if Progress is sent between an H.323 entity and a Gateway.

6.7.7.5 RELease COMplete

On the DMS, RELease COMplete is sent by the user or network, to indicate that:

- the equipment sending the message has released the channel (if any) and call reference
- the channel is available for re-use
- the receiving equipment shall release the channel and call reference

In H.225.0, RELease COMplete shall be sent by an H.323 endpoint to indicate release of the call whenever the H.225.0 call signalling channel is open.

Table 20 DMS RELease COMplete

Information Element	**Direction**	**Type**	**Length**
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	O	1
Cause	both	O[a]	4-5
Information Request	n-to-u	O	3
Signal	n-to-u	O	3

Information Element	Direction	Type	Length
Feature Indication	n-to-u	O	4-5
Locking Shift (%)	n-to-u	O	1
Display Text	n-to-u	O	4-*

[a] Cause is mandatory if this is the first clearing message, including when the RELease COMplete is sent as a result of an error handling condition. Otherwise, it is not included.

Table 21 H.225.0 RELease COMplete

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Cause	O[a]	1
Facility	O	8-*
Notification Indicator	O	2-*
Display	O	2-82
Signal	O	2-3
User-to-User	M	2-131

[a] Either the Cause IE or ReleaseCompleteReason in the ReleaseComplete-UUIE is required to be present.

6.7.7.6 SETUP

SETUP shall be sent by the calling entity to initiate call establishment to the called entity.

Table 22 DMS SETUP

Information Element	Direction	Type	Length
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	M	1
Bearer Capability	both	M	4-6
Channel Identification	both[a]	O	3
Progress Indicator	n-to-u	O	4
Keypad	u-to-n	O	3-34
Signal	n-to-u	M	3
Feature Activation	u-to-n	O	3-4

Information Element	Direction	Type	Length
Endpoint Identifier	n-to-u	O	3-4
Information Rate	n-to-u[b]	O	6
Calling Party Number	both	O	4-16
Calling Party Subaddress	both	O	4-23
Called Party Number	both	O	6-29
Called Party Subaddress	both	O	4-23
Redirecting Number	n-to-u	O	4-16
Transit Network Selection	u-to-n	O	6-7
Low-Layer Compatibility	both	O	4-16
High-Layer Compatibility	both	O	4-5
Locking Shift (%)	u-to-n	O	1
Operator System Access	u-to-n	O	3
Display Text	n-to-u	O	4-*
Locking Shift (%)	both	O	1
Call Appearance	[c]	O	3-4

[a] Channel ID is mandatory in the n-to-u direction.

[b] Included for packet-mode calls when notification is unconditional and in the network-to-user direction only.

[c] Call Appearance is included to identify the intercom group for an intercom call. It is included as specified in EKTS.

Table 23 H.225.0 SETUP

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Sending Complete	O	1
Repeat Indicator	F	NA
Bearer Capability	M	5-6
Extended Facility	O	8-*
Channel Identification	FFS	NA
Facility	O	8-*
Progress Indicator	F	NA
Network specific facilities	F	NA

Table 23 H.225.0 SETUP

Information Element	Type	Length
Notification Indicator	O	2-*
Display	O	2-82
Keypad facility	O	2-34
Signal	O	2-3
Calling Party Number	O	2-131
Calling Party Subaddress	O[a]	NA
Called Party Number	O	2-131
Called Party Subaddress	O[b]	NA
Repeat Indicator	F	NA
Transit Network Selection	F	NA
Low-Layer Compatibility	FFS	NA
High-Layer Compatibility	FFS	NA
User-to-User	M	2-131

a. Subaddresses are required for some circuit switched calls. They should not be used for packet based network only calls.
b. See a.

6.7.7.7 SETUP ACKnowledge

On the DMS, SETUP ACKnowledge is sent by the network to the calling user to indicate call establishment has been initiated, but will not proceed until additional information is exchanged.

In H.225.0, this message may be sent or received by an H.323 entity. Only an entity that indicates canOverLapSend in its SETUP-UUIE is required to support the SETUP ACKnowledge message

Table 24 DMS SETUP ACKnowledge

Information Element	Direct	Type	Length
Protocol Discriminator	n-to-u	M	1
Call Reference	n-to-u	M	2-3
Message Type	n-to-u	M	1
Channel Identification	n-to-u	M	3
Progress Indicator	n-to-u	O	4
Notification Indicator	n-to-u	O	3
Information Request	n-to-u	O	3
Signal	n-to-u	O	3

Information Element	Direct	Type	Length
Feature Indication	n-to-u	O	4-5

Table 25 H.225.0 SETUP ACKnowledge

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Channel Identification	FFS	NA
Progress Indicator	O	2-4
Display	O	2-82
Signal	O	2-3

6.7.7.8 STATus

On the DMS, STATus, when sent by the user, can only be in response to a STATus ENQuiry. It may be sent by the network to report certain error conditions.

In H.225.0, STATus shall be used to be in response to an unknown message or to a a STATus ENQuiry message.

Table 26 DMS STATus

Information Element	Direct	Type	Length
Protocol Discriminator	both	M	1
Call Reference	both	M	2-3
Message Type	both	M	1
Cause	both	M	4-6
Call State	both	M	3

Table 27 H.225.0 STATus

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Cause	M	4-32
Call State	M	3

Information Element	Type	Length
Display	O	2-82

6.7.7.9 STATus ENQuiry

On the DMS, STATus ENQuiry is sent by the network at any time during a call signaling connection to solicit a STATUS from the user. In H.225.0, STATus ENQuiry may be sent to request call status as described in section 8.4.2 “Status” of ITU-T H.323v2.

Table 28 DMS STATus ENQuiry

Information Element	Direct	Type	Length
Protocol Discriminator	n-to-u	M	1
Call Reference	n-to-u	M	2-3
Message Type	n-to-u	M	1

Table 29 H.225.0 STATus ENQuiry

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Display	O	2-82

6.7.7.10 NOTIFY

NOTIFY may be sent by the network (the DMS) or by an H.323 entity to indicate information pertaining to a call.

Table 30 DMS NOTIFY

Information Element	Direct	Type	Length
Protocol Discriminator	n-to-u	M	1
Call Reference	n-to-u	M	2-3
Message Type	n-to-u	M	1
Bearer Capability	n-to-u	M	4-6
Cause	n-to-u	O	4-5
Connected number	n-to-u	O	4-16
Notification Indicator	n-to-u	O	3

Information Element	Direct	Type	Length
Signal	n-to-u	O	3
Calling Party Number	n-to-u	O	4-16
Called Party Number	n-to-u	O	10
Called Party Subaddress	n-to-u	O	4-23
Redirecting Number	n to u	O	4-16
Redirection Number	n-to-u	O	6-13
Locking Shift (**%**)	n-to-u	O	1
Display Text	n-to-u	O	4-*

Table 31 H.225.0 NOTIFY

Information Element	Type	Length
Protocol Discriminator	M	1
Call Reference	M	3
Message Type	M	1
Bearer Capability	M	2-12
Notification Indicator	O	3
Display	O	2-82

6.7.8 Recommendations on Assignment of Fixed Feature Identifiers/Keywords

It is recommended that the control of Centrex IP Supplementary Services will be based on the generic Feature Key Management stimulus protocol as defined in ITU-T Q.932 by invoking Feature Activator/Feature Indicator (FA/FI) as supported on the DMS today and on the circuit switched network in North America.

At the time of this writing, a list of NI-2 features that are available on the DMS have a unique fixed identifier (ID) or a unique fixed keyword associated with them as shown in Table 32, " Fixed Feature Identifiers/Keywords Assignment" which have been proposed by the NIUF for ISDN ordering codes.
Note that some of the fixed identifiers that have already been standardized by Bellcore (57 and from 60 to 63).

Table 32 Fixed Feature Identifiers/Keywords Assignment

Identifier	Keyword	Feature Description
30	AUD	Automatic Dial
31	EBO	Executive Busy Override
32	SCS	Speed Call Short
33	SCL	Speed Call Long
34	SCU	Speed Call User
35	FC12	Conference size (12)
36	FC18	Conference size (18)
37	FC24	Conference size (24)
38	FC30	Conference size (30)
39	ICM	Intercom (EKTS)
47	PRK	Call Park
48	CIDSDLV	Calling Identity Delivery
49	CIDSSUP	Calling Identity Suppression
50	MSB	Make Set Busy
53	CPU	Call PickUp
54	FC6	Conference size (6)
56	ACB	Automatic CallBack

Table 32 Fixed Feature Identifiers/Keywords Assignment

Identifier	**Keyword**	**Feature Description**
57	CFU	Call Forwarding Universal
58	BCEA	Bridge Call Exclusion Activate (EKTS)
59	BCED	Bridge Call Exclusion Deactivate (EKTS)
60	FC3	Conference size (3)
61	TRANSFER	Transfer
62	DROP	Drop
63	MWI	Message Waiting Indicator/Deactivate

6.8 Real-Time Transport Protocol (RTP)

The Real-Time Transport Protocol (RTP) works in conjunction with RTCP and shares the same RFC (1899) that defines RTCP. RTP provides an end to end delivery service for data with real-time characteristics like interactive audio. Those services include payload type ID, sequence numbering, timestamping, and delivery monitoring. RTP also supports data transfers to multiple destinations using multicast distribution if provided by underlying protocol layers.

Table 33 RTP Fixed Header Format

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
v=2		P	X	CC				M	PT							Sequence Number															
Timestamp																															
Synchronization Source (SSRC) identifier																															
Contributing Source (CSRC) Identifiers																															

The first twelve octets are present in every RTP packet. The CSRC identifiers are only present when inserted by a mixer.

version (V): 2 bits

Identifies the version of RTP being used. Currently set to 2. Version 1 was the Draft version of RTP.

Padding (P): 1 bit

Set to 1 when one or more padding octets are at the end of the packet (not part of the payload). The last octet of the padding contains a count of how many padding octets should be ignored.

Extension (X): 1 bit

Set to one when the fixed header is followed by exactly one header extension.

CSRC count (CC): 4 bits

The number of CSRC identifiers that follow the fixed header.

Marker (M): 1 bit

The interpretation of the marker bit is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. A profile may also define additional marker bits or specify that there is no market bit by changing the number of bits in the payload type field.

Payload Type (PT): 7 bits

Identifies the format of the payload and determines its interpretation by the application. A profile specifies a default static mapping of payload types codes to payload formats.

Sequence Number: 16 bits

The sequence number increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence. The initial value is random to make plain text attacks on encryption more difficult, even if the source does not encrypt, since it may go through a translator that does.

Timestamp: 32 bits

Specifies the sampling instant of the first octet in the RTP packet. The initial value of the timestamp is random as is the sequence number.

SSRC: 32 bits

Identifies the synchronization source. This identifier is chosen randomly, with the intent that no two synchronization sources within the same RTP session will have the same SSRC identifier. If a source changes its source transport address, it must also choose a new SSRC identifier to avoid being interpreted as a looped source.

CSRC list: 0 to 15 items, 32 bits each

Identifies the contributing sources for the payload in the packet. The number of identifiers is given by the CC field. If there are more than 15 sources, only 15 will be identified. CSRC identifiers are inserted by mixers, using the SSRC identifiers of contributing sources.

6.8.1 FRF.11 and DTMF

DTMF transmission is frequently required to access Voice Mail servers and Interactive Voice Response (IVR) applications. Frame Relay Implementation Agreement 11 (FRF.11) provides a Dialed Digit Transfer Syntax which can be included in the RTP media stream to transfer DTMF from an IP endpoint to whatever is requesting DTMF input. The Dialed Digit Payload Format is used by the Voice over Frame Relay Sub-Frame.

6.8.1.1 Sub-Frame Format

Each sub-frame consists of a header and a payload. In the case of DTMF, the payload is in the Dialed Digit Payload Format. The minimum sub-fame header is a single octet, with the header being variable in length.

Figure 6 Sub-Frame Format

7	6	5	4	3	2	1	0
EI	LI	Sub-Channel Identification (CID) (Least Significant 6 Bits)					
CID (MSB)	0	0	Payload Type (for DTMF payload type is 0001)				
Payload Length							
Payload							

Extension Indication (EI) - The extension indication (EI) bit is set when a sub-channel identification value is >63 or when a payload type is indicated. Each transfer syntax has an implicit payload type of zero when the EI bit is cleared.

Length Indication (LI) - The Length Indication (LI) bit of the last sub-frame contained within a frame is always cleared and the payload is not present. The LI bit is set in all sub-frames preceding the last sub-frame.

Sub-Channel Identification - A zero value in the two most significant bits is implied when the EI bit is cleared. Sub-Channel identifiers 00 through 11 are reserved.

Payload Type - While there are 5 payload types, DTMF requires only one with a value of 0001.

Payload Length - Payload length contains the number of payload octets following the header. A payload length indicates the presence of two or more sub-frames packed in the information field of the frame.

Payload - The payload contains octets of a type indicated by the payload type.

6.8.1.2 Dialed Digit Payload Format

Figure 7 Dialed Digit Payload Format

<table>
<tr><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td colspan="8">Sequence Number</td></tr>
<tr><td colspan="3">Reserved (000)</td><td colspan="5">Signal Level</td></tr>
<tr><td colspan="3">Digit Type [0]</td><td colspan="5">Edge Location [0]</td></tr>
<tr><td colspan="3">Reserved (000)</td><td colspan="5">Digit Code [0]</td></tr>
<tr><td colspan="3">Digit Type [0</td><td colspan="5">Edge Location [-1]</td></tr>
<tr><td colspan="3">Reserved (000</td><td colspan="5">Digit Code [-1]</td></tr>
<tr><td colspan="3">Digit Type [0</td><td colspan="5">Edge Location [-2]</td></tr>
<tr><td colspan="3">Reserved (000</td><td colspan="5">Digit Code [-2]</td></tr>
</table>

Sequence Number - The Sequence Number field wraps from all ones to all zeroes. Each increment of the sequence number represents 20 ms.

Signal Level -The power level of each frequency is between 0 to -31 dBm0. Power levels above zero dBm0 are coded 00000. In the event that one dialed digit payload contains a transition from one dialed digit to another dialed digit, the signal level applies to the dialed digit in the “current” 20 ms period.

Figure 8 Signal Level

Code	Power Level (dBm0)
00000	0
00001	-1
00010	-2
00011	-3
00100	-4
00101	-5
00110	-6
00111	-7
01000	-8
01001	-9
01010	-10
01011	-11
01100	-12
01101	-13
01110	-14
01111	-15
10000	-16
10001	-17
10010	-18
10011	-19
10100	-20
10101	-21
10110	-22
10111	-23
11000	-24
11001	-25
11010	-26
11011	-27
11100	-28
11101	-29
11110	-30
11111	-31

Digit Type- A 20ms window is used to encode the edge when a digit is turned on and off. Digit Type is the delta time between 0ms and 19 ms, from the beginning of the current frame. If no transitions occur, the edge location will be set to 0, and the Digit Type of the previous window will be re-transmitted.

Figure 9 Digit Types

Code	Digit Type
000	Digit Off
001	DTMF On
010-111	Reserved

Digit Code - The following DTMF digit codes are encoded when the dialed digit type=DTMF=ON

Figure 10 DTMF Digit Codes

Digit Code	DTMF Digit
00000	0
00001	1
00010	2
00011	3
00100	4
00101	5
00110	6
00111	7
01000	8
01001	9
01010	*
01011	#
01100	A
01101	B
01110	C
01111	D
10000-11111	Reserved

6.8.1.3 Dialed Digit Procedures

6.8.1.3.1Transmission of Dialed Digits

When the transmitter has dialed digit data to send, it will start sending a Dialed Digit Payload every 20ms. Since each payload covers 60ms of Digit on/off edge information, there is a redundancy of the edge information. The sequence number is incremented by one in each transmitted payload.

6.8.1.3.2 Interpreting Received Dialed Digit Payloads

When a receiver accepts a Dialed Digit Payload it will generate digits according to the location of the on and off edges. Silence will be applied to the duration after an off edge and before an on edge. Digits will be generated after an on edge and before an off edge.

If the sequence number is one greater than the last received sequence number, the receiver appends the current edge information to the previous received information.

If the sequence number is two greater than the last received sequence number, the receiver appends the recent and current edge information to the previously received information.

If the sequence number is more than three greater than the last received sequence number, the receiver appends the previous, recent and current edge information to the previously received information. It fills the gap with the static values based on the previously received payload.

On a given sub-channel, if a voice payload is received at any time, an off edge should be appended to the previously received digits on/off information.

6.9 Real-Time Transport Control Protocol (RTCP)

The Real-Time Transport Control Protocol (RTCP) is defined by RFC 1889 and provides feedback on the quality of data distribution in conjunction with RTP. It is also related to the flow and congestion control functions of other protocols. RTCP uses periodic transmission of control packets to all participants in a call or session using UDP as the underlying protocol. UDP then multiplexes the control and data packets using different port numbers for each type of packet.

6.9.1 RTCP Functions

The primary function of RTCP is to provide feedback on the quality of transmission for other transport protocols. This is mandatory for IP multicasting but is also recommended for all environments.

RTCP has a persistent transport level identifier for an RTP source called the canonical name (CNAME). The CNAME is used to keep track of participants in a session since the SSRC identifier can change if a conflict is discovered pr a program is restarted. This function is mandatory for IP multicasting but is also recommended for all environments.

The first two functions described above, require all participants in a session to send RTCP packets to all other participants so each can independently monitor the number of participants in the call. This number is used to calculate the rate at which the RTCP packets are sent so RTP can scale up to large numbers of participants. Again, this function is mandatory for IP multicasting but is also recommended for all environments.

The fourth function is optional and conveys minimal session control information. This is most useful in loosely controlled sessions where participants enter and leave without membership control or parameter negotiation. RTCP is capable of reaching all participants in a call, but can not support all the control communication requirements of an application. A higher level session control protocol may be needed.

6.9.2 RTCP Packet Format

There are several RTCP packet types which carry a variety of control information. These include:

SR: Sender report for transmission and reception statistics from participants that are active members.

RR: Receiver report for reception statistics from participants that are not active senders.

SDES: Source description items, including CNAME.

BYE: Indicates the end of participation.

APP: Application specific functions.

Each RTCP packet begins with a fixed header similar to that of RTP packets.It is followed by structured elements of variable length, but which always end on a 32 bit boundary.Multiple RTCP packets may be concatenated without separators to form a compound RTCP packet that is sent in a single packet of the lower layer protocol (UDP). Lower layer protocols provide an overall length of the packet to determine the end of the compound packet so there is no need for a count of the individual packets within the compound packet.

Each individual packet within a compound packet may be processed independently with no requirement for the order or combination of packets within the following restraints:

Reception statistics (SR or RR) should be sent as often as bandwidth allows to maximize the resolution of the statistics. Each periodically transmitted compound RTCP packet should include a report packet.

Each compound packet should include the source description CNAME since new receivers need to receive the CNAME for a source as soon as possible.

The number of packet types that may appear first in the compound packet should be limited to increase the number of constant bits in the first word, and increase the probability of successfully validating RTCP packets against misaddressed RTP or other unrelated packets.

All RTCP packets must be sent in a compound packet of at least two individual packets, with the following format:

Figure 11 RTCP Compound Packet

R	{SR | #sender #site#site}	{SDES	#CNAME PHONE	#CNAME LOC}	{BYE##why}
R	{ # Report #1 #2 }	{#	#	#}	{##}
R	{#}	{#	#	#}	{##}
R	{#}	{#	#	#}	{##}

R: Encryption prefix. Only if the compound packet is to be encrypted, it is prefixed by a random 32 bit integer redrawn for every compound packet transmitted.

SR or RR: The first packet in the compound packet must be a report packet to facilitate header validation.

Additional RR's: If the number of sources for which statistics are being reported exceeds 31, then additional RR packets should follow the initial report.

SDES:An SDES packet containing the CNAME must be included in each compound RTCP packet.

BYE: The last packet to be transmitted with a given SSRC/CSRC

Chapter 7: Audio Applications

7.1 Introduction

7.1.1 General

Multiple audio applications are referred to in the H.323/H.225.0 Protocol Stack. A subset of these applications will be support by the DMS-100 internet Services in Release NA011.

7.2 Audio Packetization

7.2.1 G.711

Please refer to ITU-T Recommendation G.711, for details of that coding scheme.

7.2.2 G.723.1

This Recommendation specifies a coded representation that can be used for compressing speech signals at a very low bit rate. A G.723.1 frame can be one of three sizes: 24 bytes (6.3 Kbps frame), 20 bytes (5.3 Kbps frame), or 4 bytes. The 4 byte frames are called SID (Silence Insertion Descriptor) frames and are used to specify comfort noise parameters. There is no restriction on how 4, 20, and 24 byte frames are intermixed. The least significant two bits of the first octet in the frame determine the frame size and codec type. Switching between two frame rates can be done at any 30 ms frame boundary. Both the 20 byte and 24 byte rates are mandatory parts of the encoder and decoder. This coder was optimized to represent speech with near toll quality at the rates defined above using a limited amount of complexity.

For additional details please refer to ITU-T Recommendation G.723.1.

7.2.3 G.729A

Recommendation G.729A is a complexity reduced version of the algorithm defined in Recommendation G.729. That recommendation specifies a coded representation that can be used for compressing speech signals at a 8 Kbps bit rate. This coder was optimized to represent speech with toll or wireline qulaity at 8 Kbps. This coder has an inherent robustness against random bit errors, as well as against randomly and bursty erased frames.

For additional details please refer to ITU-T Recommendation G.729A.

List of terms

ASK	Amplitude Shift Keying
ACB	Automatic Call Back
ACO	Additional Call Offering
AE	Application Entity
Ai	Action indicator
ASP	Assignment Source Point
AT	Abstract Terminal
AUD	Automatic Dial
AUL	Automatic Line
BBG	Basic Business Group
BC	Bearer Capability
BRI	Basic Rate Interface

BS	Bearer Service
CA	Call Appearance
CACH	Call Appearance Call Handling
CAR	Call Appearance Reservation
CBQ	Call Back Queuing
CCITT	International Telegraph and Telephone Consultative Committee
CCR	Customized Code Restriction
CDN	Called Party Number
CES	Connection Endpoint Suffix
CF	Call Forward
CFAC	Call Forward All Calls
CFB	Call Forward Busy
CFC	Call Forward Cancel
CFD	Call Forward Don't Answer
CDS	Called Party Subaddress
CFF	Call l Forward Fixed

CFI	Call Forward Intergroup
CFI	Call Forward Intragroup
CFP	Call Forward Programming
CFRA	Call Forward Remote Access
CFU	Call Forward Universal
CFV	Call Forwarding Variable
CFWVAL	Call Forward Validation
CGN	Calling Party Number
CGS	Calling Party Subaddress
CHG	Charge Number
CID	Channel identification
CIDCW	Caller Identity Delivery On Call Waiting
CIDS	Calling Identify Delivery and Suppression
CLID	Caller ID
CLASS	Custom Local Area Signalling Services
CM	Computing Module

CMD	Circuit-Mode Data
CN	Connected number
CNAMD	Calling Name Delivery
CND	Calling Number Delivery
CNDA	Calling Number Delivery Activation
CNDB	Calling Number Delivery Blocking
CNDD	Calling Number Delivery Deactivation
CNI	Calling Number Identification
CNIS	Calling Number Identification Services
CNP	Calling Number Privacy
COT	Customer Originated Trace
CPE	Customer Premises Equipment
CPS	Calling Party Subaddress
CPU	Call PickUp
CR	Call Reference
CRA	Call Request Activation

CRB	Call Reference Busy
CRBL	Call Reference Busy Limit
CRd	Call Reference dummy or null
CT	Call Type
CUG	Closed User Group
CWT	Call Waiting
DC	Direct Call
DCA	Dialed Access Codes
DCPK	Directed Call Park
DDD	Direct Distance Dialing
DDO	Direct Dialing Overseas
DIN	Denied Incoming
DISA	Direct Inward System Access
DISC	Disconnect
DLH	Distributed Line Hunt
DM	Disconnected Mode

DN	Directory Number
DND	Directory Number Dependent
DND	Do Not Disturb
DNH	Directory Number Hunt
DOR	Denied Origination
DRCW	Distinctive Ringing Call Waiting
DSL	Digital Subscriber Line
DT	Display Text
DTE	Data Terminal Equipment
EBO	Executive Busy Override
EBX	Executive Busy Override - Exempt
EID	Endpoint IDentifier
EKTS	Electronic Key Telephone Service
ERWT	Expensive Route Warning Tone
ESB	Emergency Service Bureau
EXB	Extension Bridging

FA

Feature Activation

FA

Feature Activator

FC

Feature Code

FC

Flexible Calling

FCA

Feature Code Access

FCM

Functional Call Management

FCS

Frame Check Sequence

FFM

Functional Feature Management

FI

Feature Indication

FI

Feature Indicator

FIT

Fully Initializing ISDN Terminal

FKA

Feature Key Access

FKM

Feature Key Management

FPE

Feature Processing Environment

FRMR

Frame Reject

FTM

Functional Terminal Management

GIC	Group Intercom
HLC	High Layer Compatibility
HMI	Human-Machine Interface
I	Information
I-CF	ISDN Call Forwarding
I-CND	ISDN Called Number Delivery
IBN	Integrated Business Network
ICM	Intercom
IE	Information Element
IP	Internet Protocol
IRQ	Information Request
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union -Telecommunication Standardization Sector
KP	KeyPad
KSH	Keyset Short Hunt
LAPB	Link Access Procedure - Balanced

LDN

Listed Directory Number

LLC

Low-Layer Compatibility

LNR

Last Number Redial

LNRA

Last Number Redial Associated

LPIC

Preferred intraLATA Carrier

LS

Locking Shift

LSB

Least Significant Bit

LTID

Logical Terminal IDentifier

LVM

Leave Message

MADN

Multiple Appearance Directory Number

MBCE

Manual Bridged Call Exclusion

MBS

Meridian Business Set

MCA

Multiple Call Arrangement

MCH

Malicious Call Hold

MDC

Meridian Digital Centrex

MLH

Multi-Line Hunt

MRFM	MADN Ring Forward Manual
MSB	Make Set Busy
MSB	Most Significant Bit
MWT	Message Waiting
NBL	Notification Busy Limit
NCOS	Network Class of Service
NCP	Network Control Program
NDM	Normal Disconnect Mode
NI	Notification Indicator
NIT	Non-Initializing Terminal
NOAMA	No Automatic Message Accounting
NPI	Number Plan Identification
NPSI	Network Control Packet Switching Interface
NRM	Normal Response Mode
NRS	Network Resource Selector
NT	Network Termination

NT1	Network Termination Equipment
NTMFT	Nortel Meridian Feature Transparency
NTTRF	Nortel Bellcore TR-compliant Functional
OM	Operation Measurement
OSA	Operator System Access
PBX	Private Branch Exchange
PCA	Privacy Change Allowed
PCM	Pulse Code Modulation
PD	Parameter Downloading
PDN	Primary DN
PH	Packet Handler
PI	Progress Indicator
PIC	Preferred interLATA Carrier
PMD	Packet Mode Data
PPSN	Public Packet Switched Network
PRK	Call Park

PS	Packet Switched
PSDS	Public Switched Digital Service
PVC	Protocol Version Control
QLLC	Qualified Logical Link Control
RAG	Ring Again
REJ	Reject
RES	Residential Enhanced Services
RF	Ring Forward
RGN	Redirecting Number
Ri	Reference number
RLS	Release
RN	Redirecting Number
RND	Redirecting Number Display
RNN	Redirection Number
RNR	Receive Not Ready
RO	Remote Operations

ROSE	Remote Operations Service Element
RR	Receive Ready
RU	Remote Unit
S	Supervisory
SABME	Set Asynchronous Balanced Mode Extended
SAP	Service Access Point
SAPI	Service Access Point Identifier
SC	Speed Call
SCA	Selective Call Acceptance
SCA	Single Call Arrangement
SCF	Selective Call Forwarding
SCL	Speed Call - Long list
SCP	Signalling Control Protocol
SCR	Selective Call Rejection
SCS	Speed Call - Short list
SCU	Speed Call User

SDLC	Synchronous Data Link Control
SDN	Secondary DN
SERVORD	Service Orders
SIG	Signal
SLE	Screen List Editing
SLU	Subscriber Line Usage
SNA	System Network Architecture
SPID	Service Profile Identifier
SPM	Service Profile Management
SSRT	Station Ringing Transfer
SVC	Switched Virtual Circuit
TBD	To be Determined
TCA	Terminal Call Appearance
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
TID	Terminal IDentifier

TN/NPI	Type of Number/Numbering Plan Indicator
TNS	Transit Network Selection
TON	Type Of Number
TRC	Terminating Restriction Code
TSP	Terminal Service Profile
UA	Universal Access
UA	Unnumbered Acknowledgment
UCD	Uniform Call Distribution
UI	Unnumbered Information
UP	User Provided
USID	User Service Identifier
VI	Voiceband Information
VO	Verification Office
WAN	Wide Area Network
WML	Warm Line
XID	Exchange Identification

XPM

Extended Peripheral Module

Bibliography

"Voice Over Packet-Network GatewayDesign Specification", DS7X07AA, Stream 1A, Issue 05, September 11, 1998, Northern Telecom, Inc.

"NA011 Internet Telephony Services Feature Specification Document", ITSFSD, Version AA04, January 14, 1998, Northern Telecom Inc.

"ISDN Basic Rate User Network Interface Specification", NIS-S208-6, Issue 03.01, Northern Telecom, Inc., September, 1997

ITU-T Recommendation H.323, ITU-T Study Group 16, 1998, Packet Based Multimedia Communications Systems

ITU-T Recommendation H.225.0,Version 2, March 25,1997 ITU-T Study Group 15, 1997, Call Signaling Protocols and Media Stream Packetization for Packet based Multimedia Communications Systems.

"RTP: A Transport Protocol for Real-Time Applications", RFC 1889, H.Schulzrinne,S. Casner,R. Frederick, V.Jacobson, January 1996.

"Transmission Control Protocol", RFC793, J. Postel, Sept. 1, 1981

Interworking with TCP/IP, Volume 1, D. Comer, Prentice Hall, ISBN 0-13-216987-8

Centrex IP Services

NIS-S227-1

Issue 01.02

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks Corporation. Except as specifically authorized in writing by Nortel Networks, the holder shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only.

Information subject to change without notice.

Document name: Centrex IP Services Network Interface Specification
Document Number: NIS-S227-1
Document Date: September 1999
Document Issue: Issue 01.02
Security status: Public

The following are trademarks of Nortel Networks: Bell-Northern Research, DMS-100, Nortel , Meridian, Centrex IP.

NORTEL NETWORKS™