Iridium RUDICS Description and VAR Interface Guide

Release 1.0
January 23, 2004

Iridium Satellite LLC Confidential & Proprietary Information

.

Ver	Description	Date	Author
1.0	Initial document	10/30/02	Kent Keeter

Table of Contents

1.0 Introduction

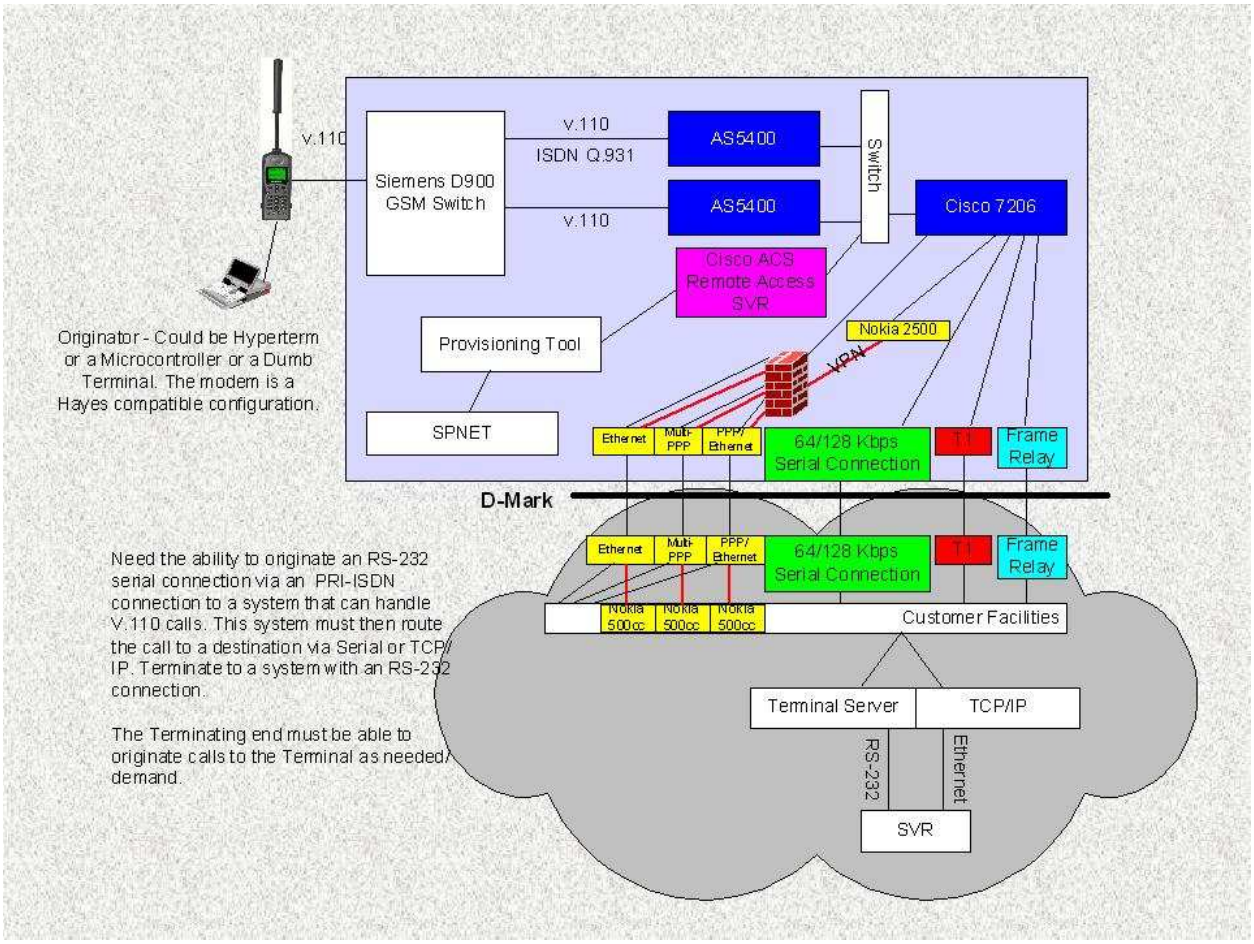
The purpose of this document is to provide information for the different connectivity capabilities of the RUDI-CS system in the Iridium system. This document shows the system as a whole and then as a individual types of connectivity. The different types of connectivity will only show the possible scenarios based on the initial delivery of this service. Thus this is a living document and should be considered as such.

2.0 Scope

The scope of this document is to provide basic operational connectivity configurations for customers to use. This document is covering Mobile Originated (MO) and Mobile Termination (MT) Circuit Switch Data calls to the RUDI-CS' system. Features of the Mobile Originated calls include high-level data link control (HDLC), Ethernet (TCP/IP), Point-to-Point Protocol (PPP) and Multi-Link Point-to-Point Protocol (MLPP) and features for Mobile Termination of HDLC and TCP/IP will be documented here.

3.0 Production Environment

The following diagram shows the full production environment.



The above figure shows all of the possible scenarios for connectivity to the gateway. The following subsections will layout the individual types of connectivity and their capabilities.

The production environment has three main types of services: TCP/IP Encapsulation, PPP and MLPP. These types of services have multiples of configurations. This document will lay the groundwork for a customer to integrate their system onto the appropriate configuration. Below is a list of the different configurations. The RUDI-CS system is by no means limited to these configurations, as new configurations manifest, they will be added to this document.

Connectivity Types					
		Origination Types			
		Mobile			Fixed Site or SVR
		Custom Device	PPP	MLPP	Telnet Only
Termination Types	Ethernet	X	X	X	
	Ethernet VPN	X	X	X	
	T1	X	X	X	
	E1	X	X	X	
	Serial (X Kbs)	X	X	X	
	Frame Relay	X	X	X	
	ISU Device				X

3.1.1 Custom Device

A custom device is a unit that does not require a TCP/IP stack. This device needs to be capable to communicate using the RS-232 standard to the Data interface of an Iridium Subscriber Unit/Device, for example the 9500, 9505 or 9522. This device must be able to use the standard "AT" commands to communicate with the Iridium Subscriber Unit/Device.

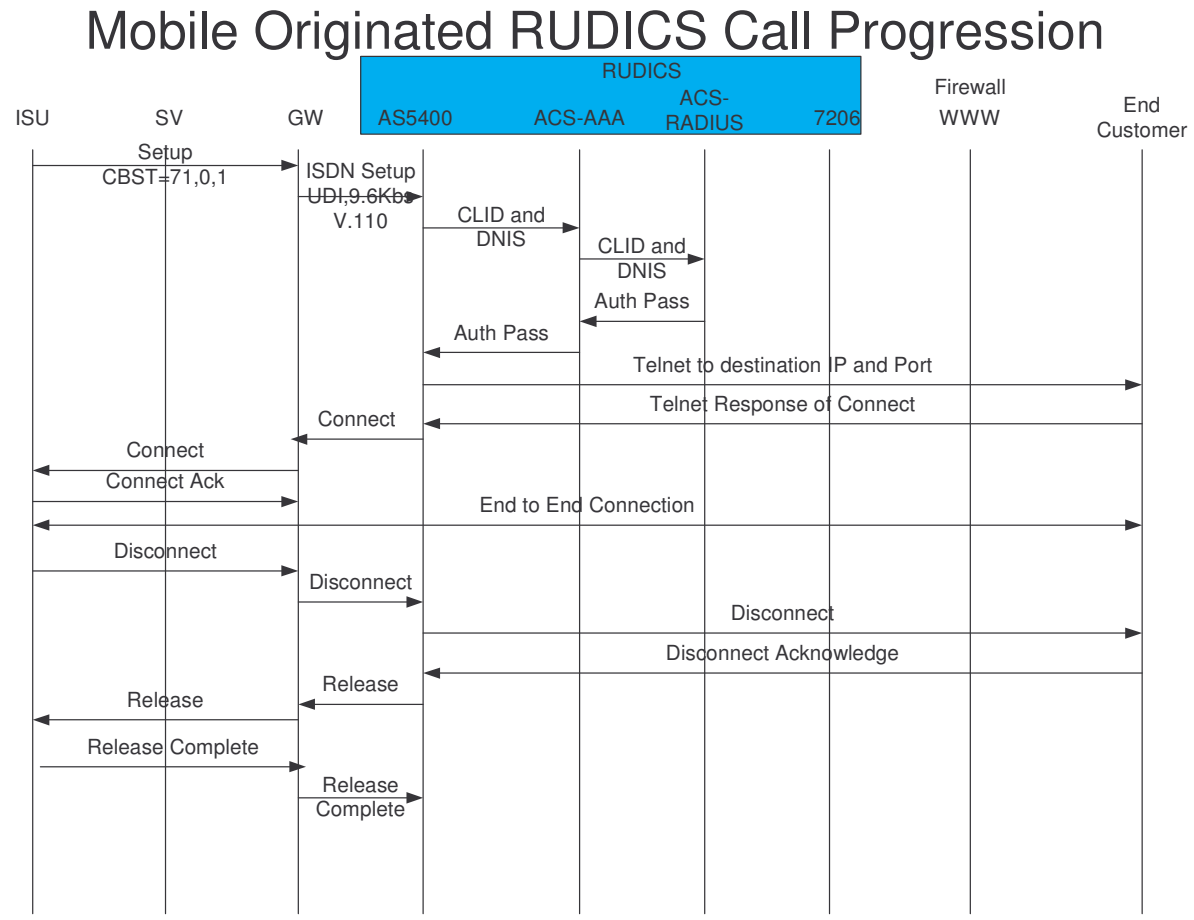
#	Description
1	Custom Device–ISU-GW-RUDICS-WWW-Terminal Server- Custom Device/Server: Allows a Custom Device without a TCP/IP Stack the capability to dial into the RUDICS system and be connected to another Custom Device Server.
2	Custom Device-ISU-GW-RUDICS-WWW-Server: Allows for a Custom Device without a TCP/IP Stack the capability to dial into the RUDICS system and be connected to a Server/Application.
3	Custom Device-ISU-GW-RUDICS-WWW (VPN)-Terminal Server-Custom Device/Server: Allows for a Custom Device without a TCP/IP stack the capability to dial into the RUDICS system and be connected to another Custom Device or Server.
4	Custom Device-ISU-GW-RUDICS-X Kbs-Terminal Server-Custom Device/Server: Allows for a Custom Device without a TCP/IP stack the capability to dial into the RUDICS system and be connected via a private X Kbs circuit to another Custom Device or Server.
5	Custom Device-ISU-GW-RUDICS-T1/E1-Terminal Server-Custom Device/Server: Allows for a Custom Device without a TCP/IP stack the capability to dial into the RUDICS system and be connected via a private T1/E1 circuit to another Custom Device or Server.
6	PC/Smart Device-ISU-GW-RUDICS-PPP-WWW: Allows a Device with a TCP/IP stack the access into the Web utilizing Peer–to-Peer Protocol (PPP).
7	PC/Smart Device-ISU-GW-RUDICS-PPP-WWW (VPN)-Server: Allows a Device with a TCP/IP stack the access into the Web via VPN to a Group Home Network utilizing Peer –to-Peer Protocol (PPP).
8	PC/Smart Device-ISUs-GW-RUDICS-MLPP-WWW: Allows a Device with a TCP/IP stack the access into the Web utilizing Multi-Link Peer –to-Peer Protocol (MLPP).
9	PC/Smart Device-ISUs-GW-RUDICS-MLPP-WWW (VPN): Allows a Device with a TCP/IP stack the access into the Web via VPN to a Group Home Network utilizing Multi-Link Peer –to-Peer Protocol (MLPP).

3.2 Mobile Origination: Call Origination from an Iridium Subscriber unit:

Using an application that can initiate "AT" commands perform the following steps to originate a call to the RUDI-CS system.
Transmit: "at+cbst=71,0,1"
Receive: "OK"
Transmit: "atdt00881600005XX" (Note: This is the Group number assigned.)
Receive: "Connect <Baud Rate>"
Note: The Baud Rate is reflected is that of the unit to the ISU and is dependent upon the unit capability.
Receive: "Trying X.X.X.X, Port … Open" (Note: the X.X.X.X, Port is the destination TCP/IP address and Port.)
Once this is received the pipe is now open for communication.

3.2.1 Call Processing of Mobile Originated

The call processing of the Mobile Originated call is displayed as below.



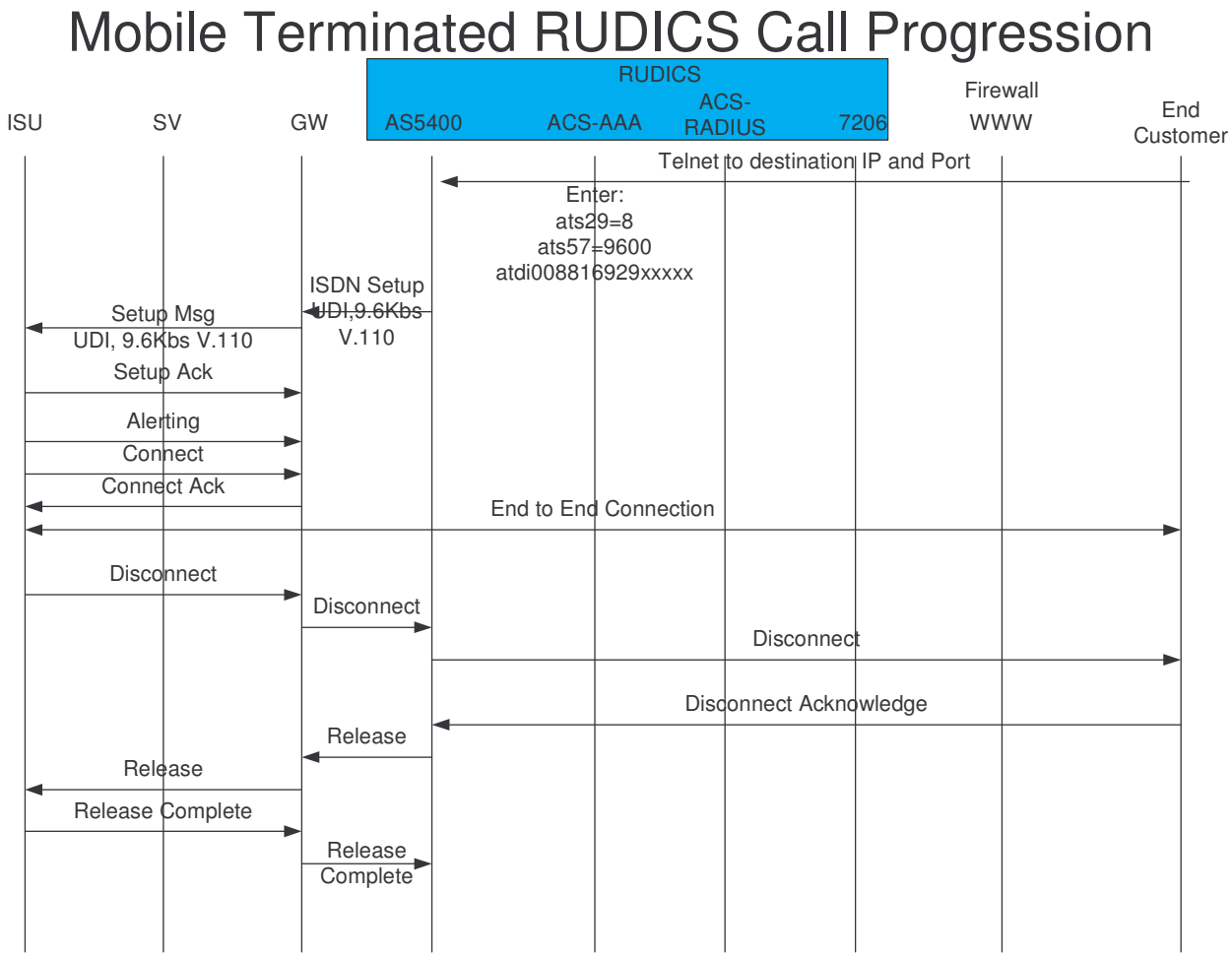
The Cisco AS5400 can also capture the call flow of a call by using the debug commands. The following information was capture by turning ISDN Q931, AAA Authentication and AAA Radius information via the debug command. The call is a Mobile Originated call and Mobile Side terminating the call and can be viewed in Appendix B.

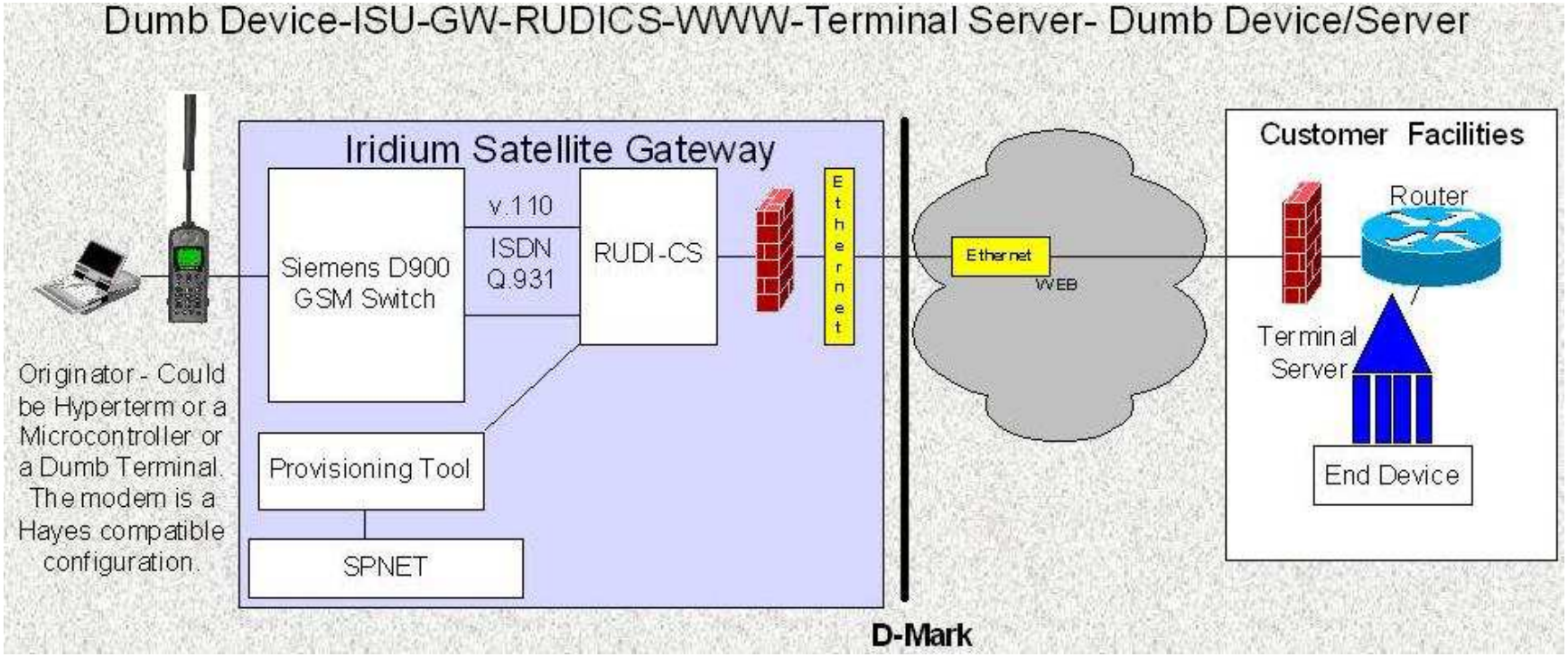
3.3 Mobile Termination: Call Origination from the Server side:

Using an application that can initiate telnet and commands within the telnet session perform the following steps to originate a call through the RUDI-CS system to an Iridium Subscriber Unit.
Transmit: “telnet X.X.X.X” (Note: The X.X.X.X will be given upon assigning the group capabilities.)
Receive: Blank Screen (Note: Telnet will know if the connection was made or not. If the connection was not established the telnet session will show the connection refused.)
Transmit: “ats29=8” (Note: This sets the call type to V.110.)
Receive: “OK”
Transmit: “ats57=9600” (Note: This sets the call speed to 9600 baud.)
Receive: “OK”
Transmit: “atdi008816929XXXXX” (Note: From the RUDI-CS system only the MSISDN-C number is enabled.)
Good Call:
Receive: “CONNECT 9600 /V110”
If Busy:
Receive: “BUSY”
If No Answer:
Receive: “No Carrier”

3.3.1 Call Processing of Mobile Terminated

The call processing of the Mobile Terminated call is displayed as below.





3.4 Dumb Device–ISU-GW-RUDICS-WWW-Terminal Server- Dumb Device/Server: Allows a Dumb Device

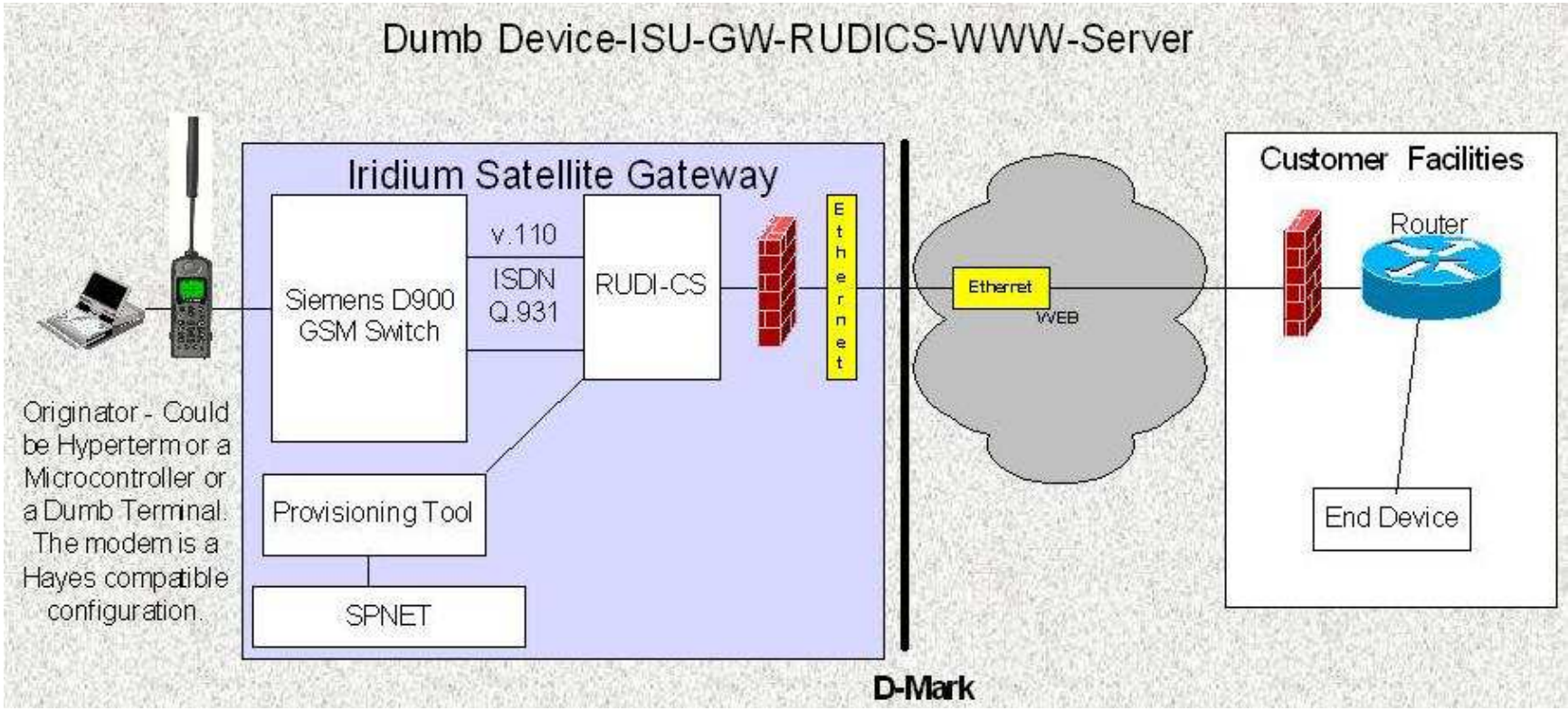
The connectivity illustrated above shows a simple connection from an end to end. This type of connectivity is designed for devices without a TCP/IP Stack. Utilizing "AT" commands an end device is able to originate and terminate a call from a Device connected to an Iridium Subscriber device. This connection also allows the Server/Device Driver from the TCP/IP end, the ability to call the end device.

From the origination side of the Iridium network a device calls the Group number assigned to the TCP/IP customer. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1". This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on "881600005XX". Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. "8816314XXXXX". The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the TCP/IP destination.
To setup up this type of connectivity the items required are as follows: Group Name, a Group Number will be assigned, TCP/IP address and Port for the Destination end, if echo is required for this connection, and if streaming is required. Once the connectivity is established members can then be added to the

group. To add a member you only need the 8816314XXXXX number (not the MSISDN-C). The only time a MSISDN-C is used, is when it is the only number assigned to the member.

Dumb Device–ISU-GW-RUDICS-WWW-Terminal Server- Dumb Device/Server	
Pros	**Cons**
No TCP/IP stack required.	No ability to originated call from Terminal Server end.
Proprietary Protocol can be used.	End device is open to what ever connects to it.
No Need for ISU to ISU type of connection	Total security of circuit is not possible through the open WWW network.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	
Ability to make several connections via Ethernet to a Terminal Server with multiple end connections.	



3.5 Dumb Device-ISU-GW-RUDICS-WWW-Server

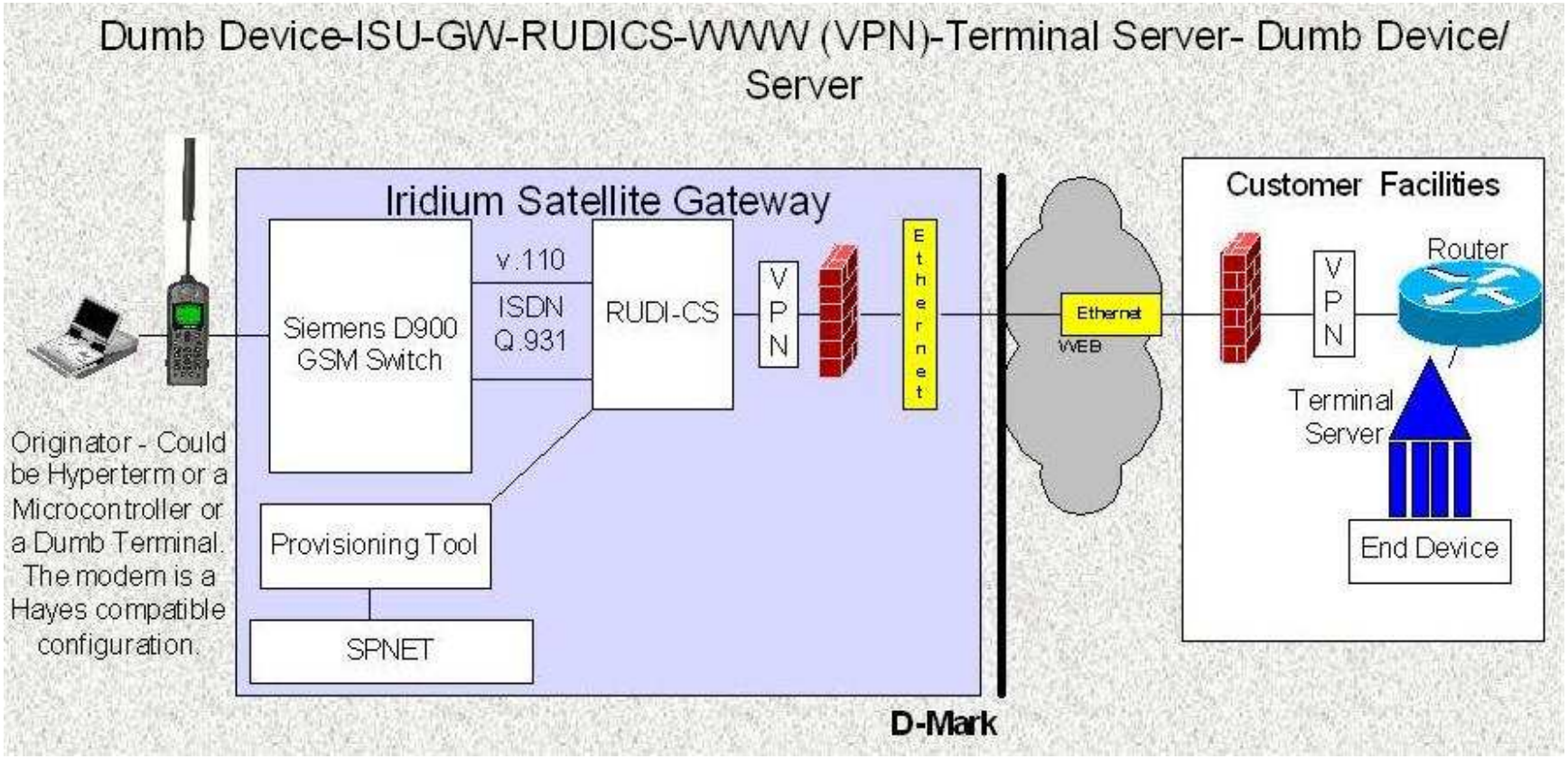
The connectivity illustrated above shows a simple connection from an end to end. This type of connectivity is designed for devices without a TCP/IP Stack to a Device that has a TCP/IP stack. Utilizing "AT" commands an end device is able to originate and terminate a call from a Device connected to an Iridium Subscriber device. This connection also allows the Server from the TCP/IP end, the ability to call the end device.

From the origination side of the Iridium network a device calls the Group number assigned to the TCP/IP customer. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1". This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on "881600005XX". Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. "8816314XXXXX". The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the TCP/IP destination.

To setup up this type of connectivity the items required are as follows: Group Name, a Group Number will be assigned, number of ports required, TCP/IP address and Port for the Destination end, if echo is required for this connection, and if streaming is required. Once the connectivity is established members can then be added to the group. To add a member you only need the 8816314XXXXX number (not the MSISDN-C). The only time a MSISDN-C is used, is when it is the only number assigned to the member.
Once the connectivity is established the client devices can call to the server destination. This calling pattern is important to monitor due to the number of ports that the Group has designated. This is established at the connectivity stage. This controls the number of connections that will be established simultaneously. It should be noted that the number of ports is for both incoming and outgoing connectivity.

Dumb Device-ISU-GW-RUDICS-WWW-Server	
Pros	**Cons**
No TCP/IP stack required for Originating end.	No ability to originated call from Terminal Server end.
Proprietary Protocol can be used.	End device is open to what ever connects to it.
No Need for ISU to ISU type of connection	Total security of circuit is not possible through the open WWW network.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	
Ability to connect to several end devices simultaneously utilizing only an Ethernet connection.	
Ability to originate calls via a Telnet session.	



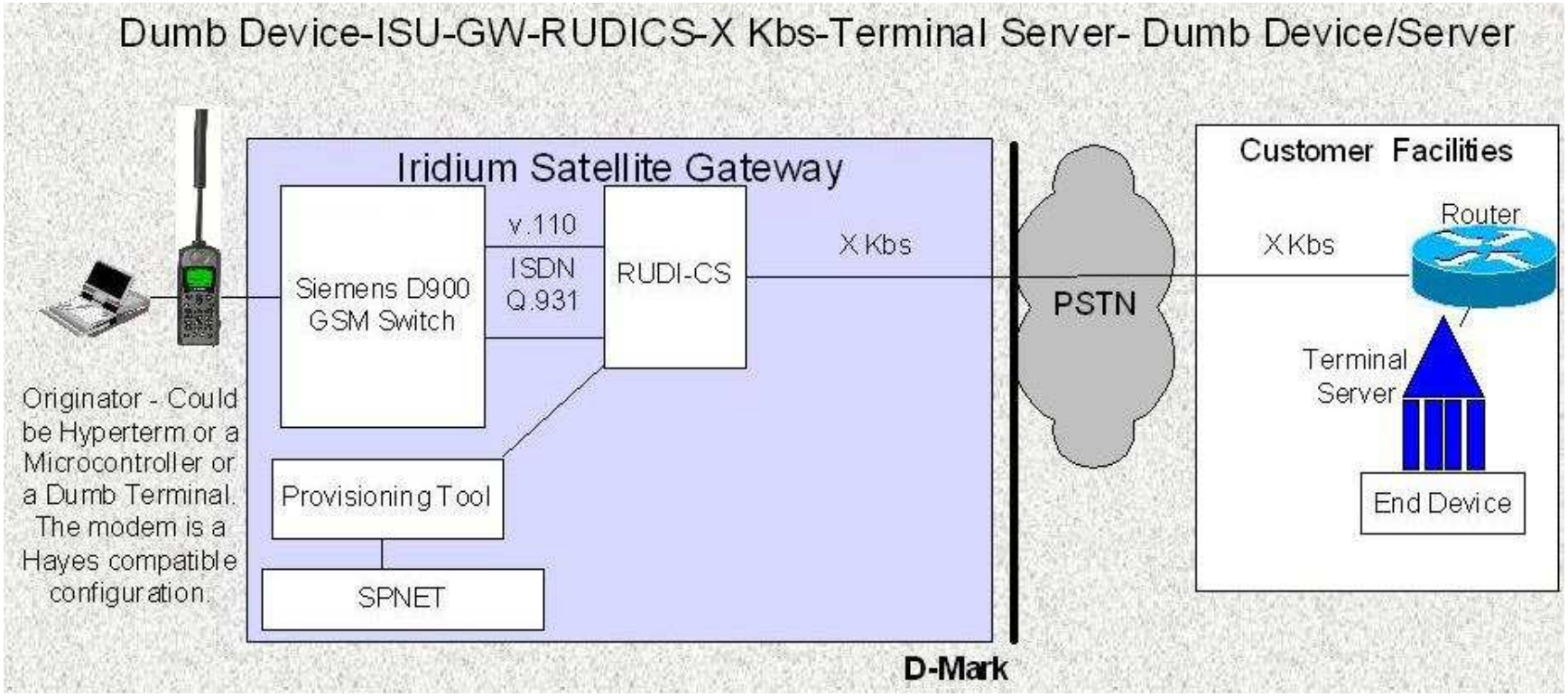
3.6 Dumb Device-ISU-GW-RUDICS-WWW (VPN)-Terminal Server-Dumb Device/Server

The connectivity illustrated above shows a simple connection from an end to end. This type of connectivity is designed for devices without a TCP/IP Stack to a Device that has a TCP/IP stack. Utilizing "AT" commands an end device is able to originate and terminate a call from a Device connected to an Iridium Subscriber device. This connection also allows the Server from the TCP/IP end, the ability to call the end device.

From the origination side of the Iridium network a device calls the Group number assigned to the TCP/IP customer. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1". This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on “881600005XX”. Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. “8816314XXXXX”. The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the TCP/IP destination.

Dumb Device–ISU-GW-RUDICS-WWW (VPN)-Terminal Server- Dumb Device/Server	
Pros	**Cons**
No TCP/IP stack required.	No ability to originated call from Terminal Server end.
Proprietary Protocol can be used.	End device is open to what ever connects to it.
No Need for ISU to ISU type of connection	
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	
Ability to make several connections via Ethernet to a Terminal Server with multiple end connections.	
The VPN adds end to end Security of the Pipe from Iridium to the Destination.	



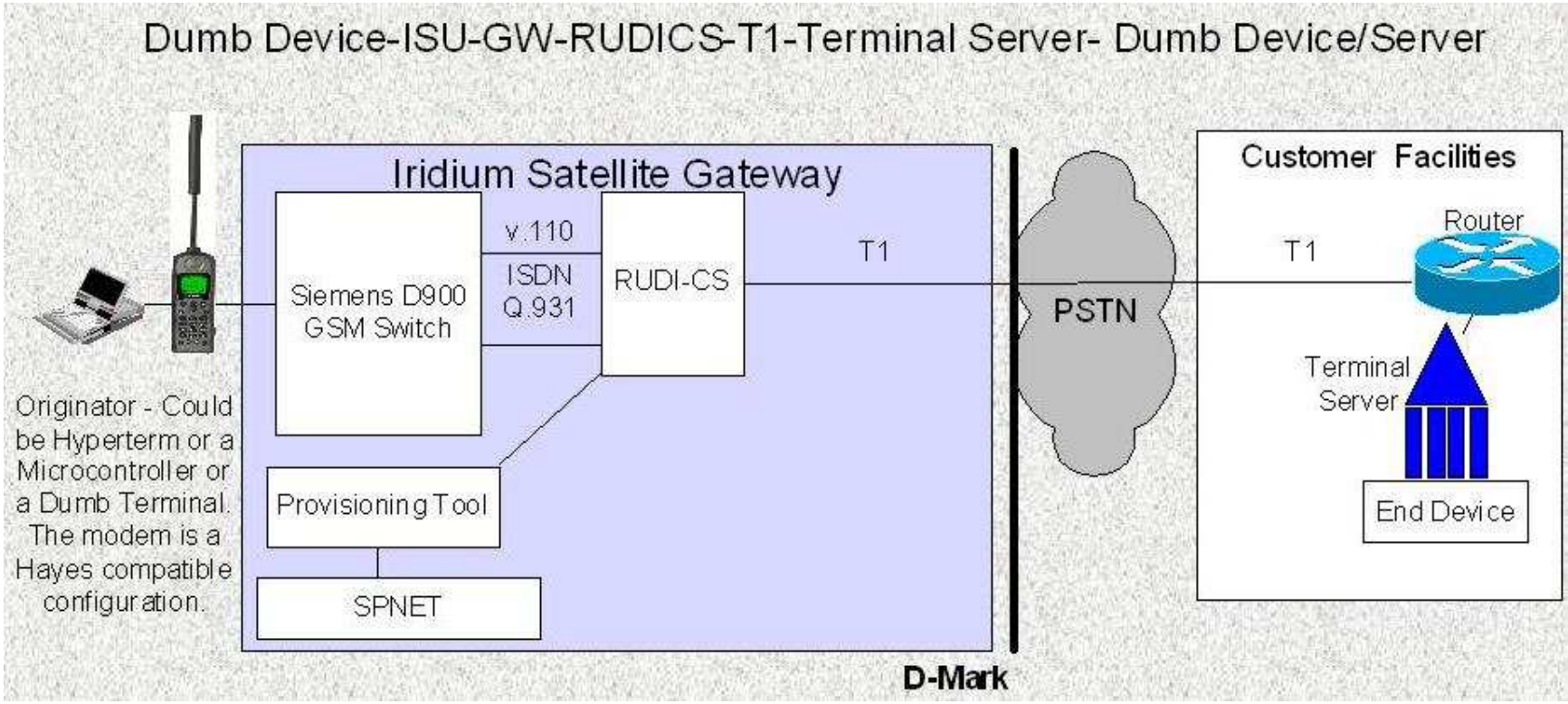
3.7 Dumb Device-ISU-GW-RUDICS-X Kbs-Terminal Server-Dumb Device/Server

The connectivity illustrated above shows a simple connection from an end to end. This type of connectivity is designed for devices without a TCP/IP Stack to a Device that also does not have a TCP/IP stack. Utilizing "AT" commands an end device is able to originate and terminate a call from a Device connected to an Iridium Subscriber device. This connection also allows the Server from a TCP/IP end, the ability to call the end device.

From the origination side of the Iridium network a device calls the Group number assigned to the TCP/IP customer. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1". This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on "881600005XX". Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. "8816314XXXXX". The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the destination.

Dumb Device-ISU-GW-RUDICS-X Kbs-Terminal Server- Dumb Device/Server	
Pros	**Cons**
No TCP/IP stack required.	No ability to originated call from Terminal Server end.
Proprietary Protocol can be used.	End device is open to what ever connects to it.
No Need for ISU to ISU type of connection	Not able to originate calls from a terminal server device currently.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	
Ability to make several connections via Ethernet to a Terminal Server with multiple end connections.	
Added security because connection does not ride the WWW the connection is point to point.	



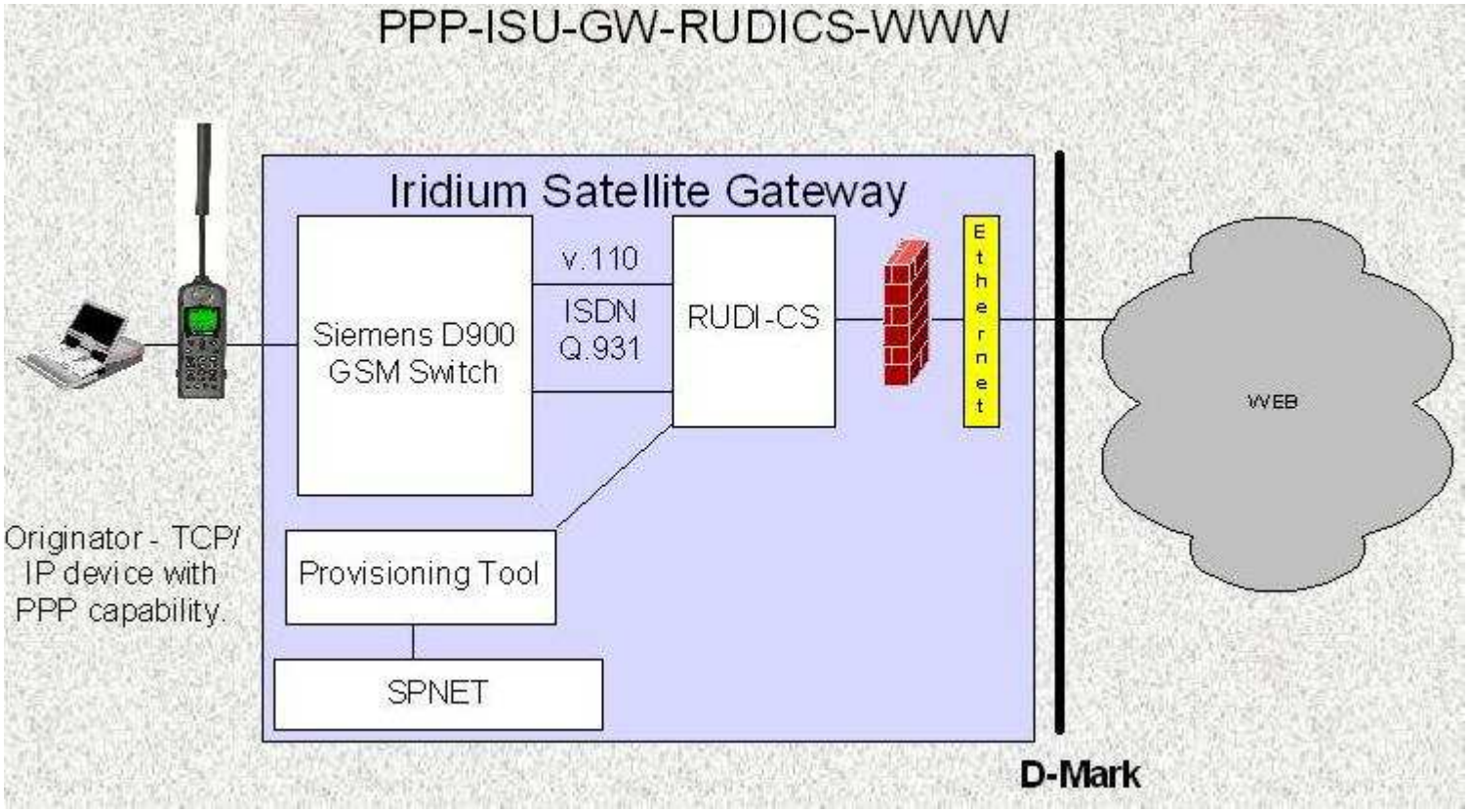
3.8 Dumb Device-ISU-GW-RUDICS-T1/E1-Terminal Server-Dumb Device/Server

The connectivity illustrated above shows a simple connection from an end to end. This type of connectivity is designed for devices without a TCP/IP Stack to a Device that also does not have a TCP/IP stack. Utilizing "AT" commands an end device is able to originate and terminate a call from a Device connected to an Iridium Subscriber device. This connection also allows the Server from a TCP/IP end, the ability to call the end device.

From the origination side of the Iridium network a device calls the Group number assigned to the TCP/IP customer. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1". This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on "881600005XX". Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. "8816314XXXXX". The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the destination.

Dumb Device-ISU-GW-RUDICS-X Kbs-Terminal Server- Dumb Device/Server	
Pros	**Cons**
No TCP/IP stack required.	No ability to originated call from Terminal Server end.
Proprietary Protocol can be used.	End device is open to what ever connects to it.
No Need for ISU to ISU type of connection	Not able to originate calls from a terminal server device currently.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	
Ability to make several connections via Ethernet to a Terminal Server with multiple end connections.	
Added security because connection does not ride the WWW the connection is point to point.	



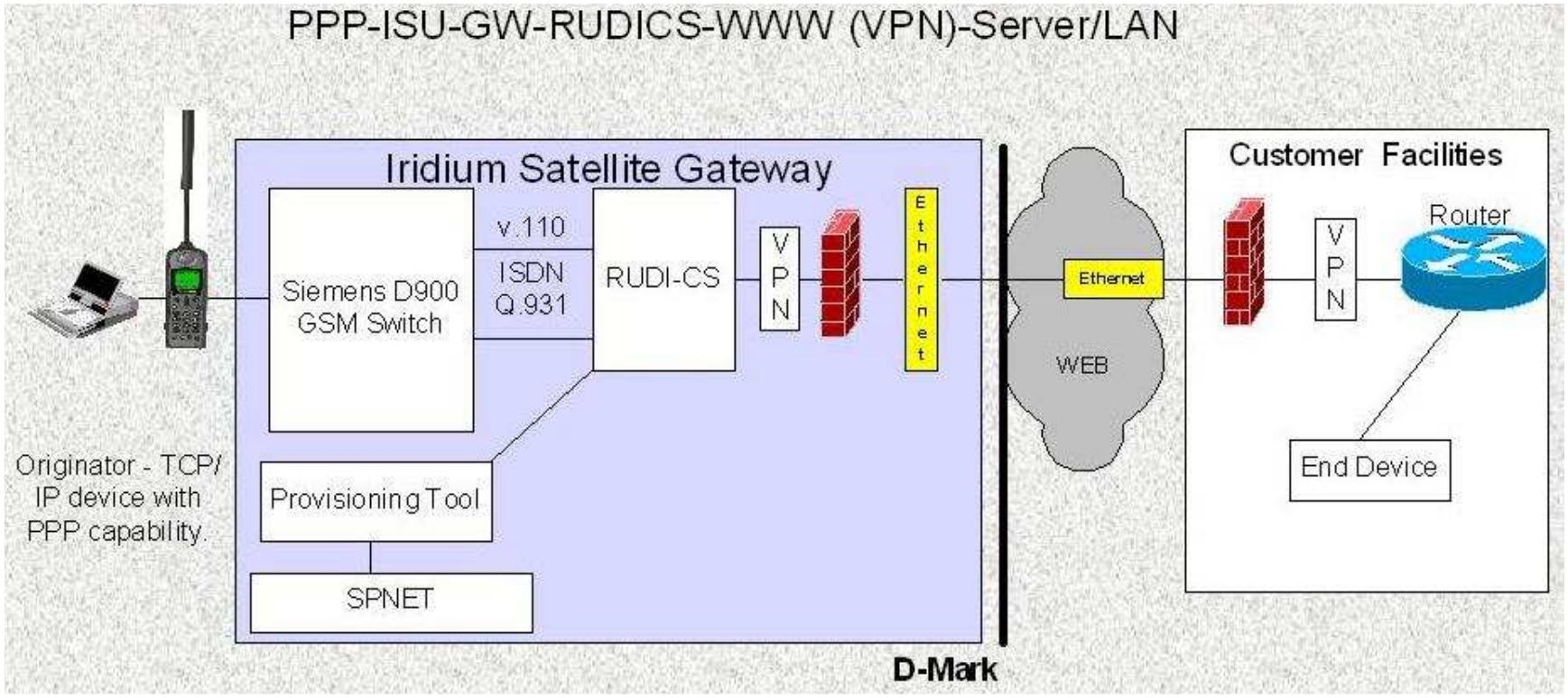
3.9 PC/Smart Device-ISU-GW-RUDICS-PPP-WWW

The connectivity illustrated above shows a simple connection from an end to the web. This type of connectivity is designed for devices with a TCP/IP Stack to the World Wide Web (WWW). Utilizing Dial-Up Networking (for Windows types of systems) the user is able to dial the Group number and be connected to the WWW. This connection is designed for mobile originated only. Currently Mobile terminated is not possible.

From the origination side of the Iridium network a device calls the Group number assigned to the WWW. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1" and can be set up as part of the initialization of the modem driver being used. This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number.

The Group number is assigned based on “881600005XX”. Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. “8816314XXXXX”. The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the destination.

PC/Smart Device-ISU-GW-RUDICS-PPP-WWW	
Pros	**Cons**
Ability to connect to the WWW quickly.	Not able to originate calls from a terminal server device currently.
Does not require the Windows operating system.	Data rate is only 2.4.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	Compression is currently not available.



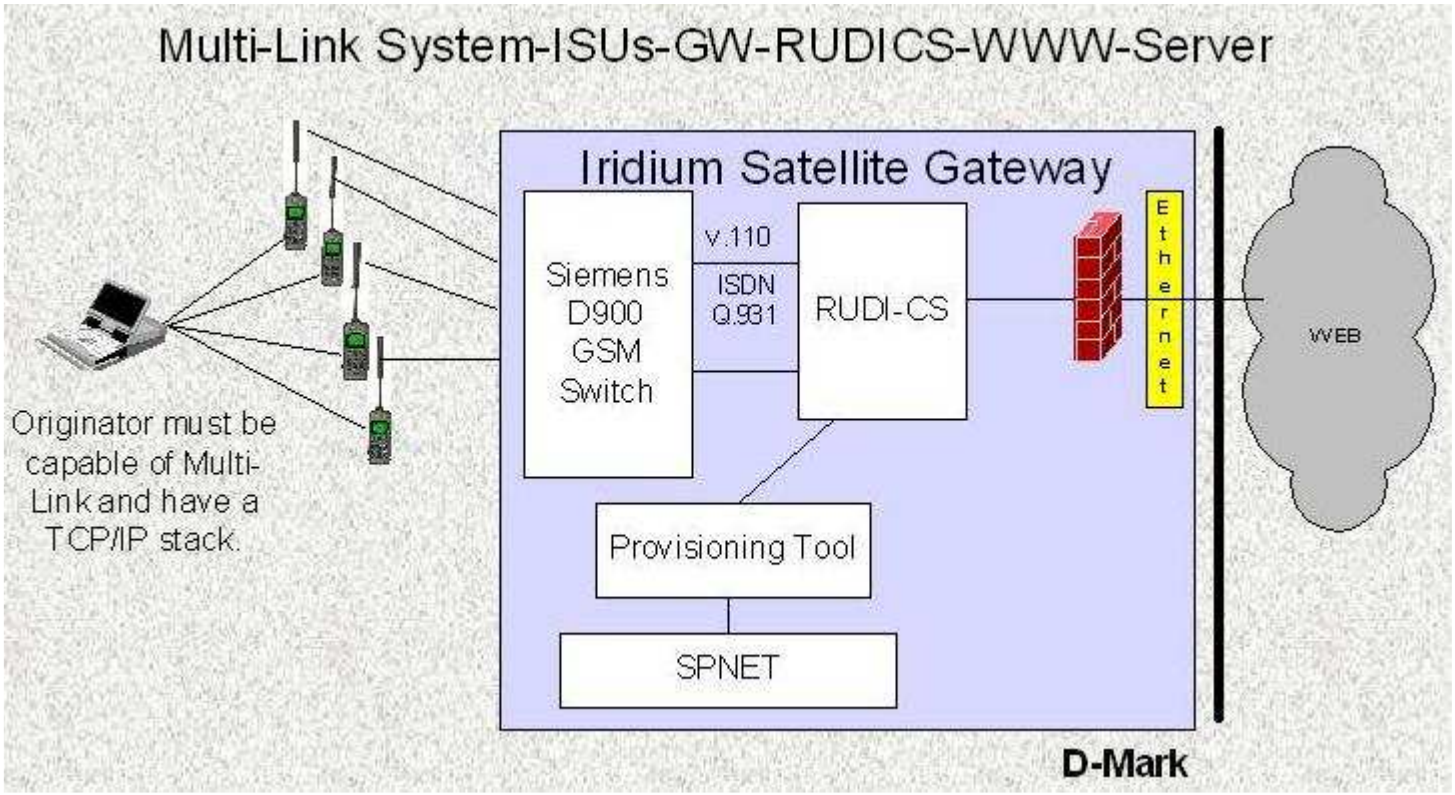
3.10 PC/Smart Device-ISU-GW-RUDICS-PPP-WWW (VPN)-Server

The connectivity illustrated above shows a simple connection from an end to a Group's Home Network. This type of connectivity is designed for devices with a TCP/IP Stack to the World Wide Web (WWW). Utilizing Dial-Up Networking (for Windows types of systems) the user is able to dial the Group number and be connected to their Home Network. This connection is designed for mobile originated only. Currently Mobile terminated is not possible.

From the origination side of the Iridium network a device calls the Group number assigned to the Group Home Network. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1" and can be set up as part of the initialization of the modem driver being used. This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number. Once the call has been validated it is then routed to the Virtual Private Network (VPN) appliance. This appliance is permanently connected to the Home Networks appliance. This ensures better connectivity and security.

The Group number is assigned based on “881600005XX”. Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. “8816314XXXXX”. The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the destination.

PC/Smart Device-ISU-GW-RUDICS-PPP-WWW (VPN)-Server/LAN	
Pros	**Cons**
Ability to connect to the WWW quickly.	Not able to originate calls from a terminal server device currently.
Does not require the Windows operating system.	Data rate is only 2.4.
Security Verification of Originating number for Destination. ONLY a member can reach the Destination by the Iridium network.	Compression is currently not available.
The VPN adds end to end Security of the Pipe from Iridium to the Destination.	



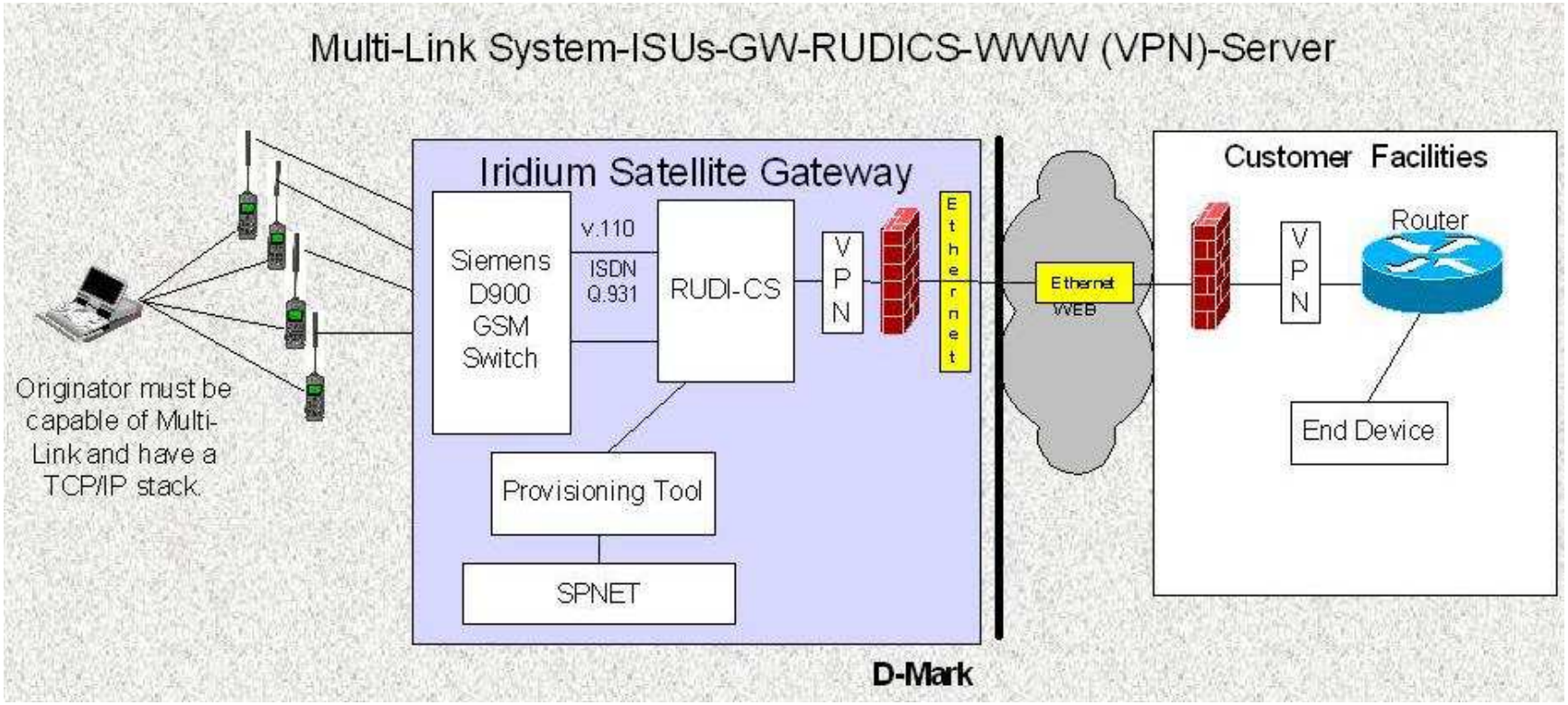
3.11 Multi-Link PPP Device-ISUs-GW-RUDICS-WWW

The connectivity illustrated above shows a simple connection from an end to the web. This type of connectivity is designed for devices with a TCP/IP Stack and the Capability of Multi-Link PPP to the World Wide Web (WWW). Utilizing Dial-Up Networking (for Windows types of systems; see Appendix A) the user is able to dial the Group number and be connected to the WWW. This connection is designed for mobile originated only. Currently Mobile terminated is not possible.

From the origination side of the Iridium network a device calls the Group number assigned to the MLPP-WWW service. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISUs as follows “at+cbst=71,0,1” and can be set up as part of the initialization of the modem driver being used. This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows “00881600005XX”. Once the calls come into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating numbers.

The Group number is assigned based on “881600005XX”. Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The members are unique phone numbers, i.e. “8816314XXXXX”. The members when dialing the Group number will be authenticated using both the Origination numbers and Termination number. This means that ONLY members of that Group will be able to reach the destination.

Multi-Link PPP Device-ISUs-GW-RUDICS-PPP-WWW	
Pros	**Cons**
Ability to connect to the WWW quickly.	Compression is currently not available.
Ability to increase the Bandwidth for the connection to the WWW at 2K+ per phone making the call.	More Iridium Devices and accessories are needed to make this type of call.
Does not require the Windows operating system.	
Security Verification of Originating number for Destination. ONLY members can reach the Destination by the Iridium network.	



3.12 Multi-Link System-ISUs-GW-RUDICS-WWW (VPN)-Server

The connectivity illustrated above shows a simple connection from an end to a Group's Home Network. This type of connectivity is designed for devices with a TCP/IP Stack to the World Wide Web (WWW). Utilizing Dial-Up Networking (for Windows types of systems; see Appendix A) the user is able to dial the Group number and be connected to their Home Network. This connection is designed for mobile originated only. Currently Mobile terminated is not possible.

From the origination side of the Iridium network a device calls the Group number assigned to the Group Home Network. To call this number the phone must be configured to make an ISDN call. This is performed by setting the Call Bearer service on the ISU as follows "at+cbst=71,0,1" and can be set up as part of the initialization of the modem driver being used. This sets the phone to make a 9600 UDI type of call. The number to be dialed looks as follows "00881600005XX". Once the call comes into the RUDI-CS system, two validations are performed. The first is the validation of the Group Number; the second is the validation of the originating number. Once the call has been validated it is then routed to the Virtual Private Network (VPN) appliance. This appliance is permanently connected to the Home Networks appliance. This ensures better connectivity and security.

The Group number is assigned based on “881600005XX”. Once the Group has been assigned the SP or controller of the account will be allowed to add users/members to the Group. The member is a unique phone number, i.e. “8816314XXXXX”. The member when dialing the Group number will be authenticated using both the Origination number and Termination number. This means that ONLY a member of that Group will be able to reach the destination.

PC/Smart Device-ISU-GW-RUDICS-PPP-WWW (VPN)-Server/LAN	
Pros	**Cons**
Ability to connect to the WWW quickly.	Compression is currently not available.
Ability to increase the Bandwidth for the connection to the WWW at 2K+ per phone making the call.	More Iridium Devices and accessories are needed to make this type of call.
Does not require the Windows operating system.	
Security Verification of Originating number for Destination. ONLY members can reach the Destination by the Iridium network.	
The VPN adds end to end Security of the Pipe from Iridium to the Destination.	

4.0 Appendix A

4.1 PPP operation and protocols

Point-to-Point Protocol (PPP) connections must adhere to standards established in PPP RFC's. This section gives an overview of PPP operations and the protocols used in a PPP connection. For information about configuring PPP settings, see PPP setting.

Dial-up sequence

After an initial connection to a remote PPP server, the following negotiations establish a PPP connection:

- Link Control Protocols (LCP)
  LCP is used to establish and configure link and framing settings such as maximum frame size.
- Authentication protocols
  Authentication protocols are used to determine what level of security validation the remote access server can perform and what the server requires. The level of security that can be negotiated ranges from unencrypted (plaintext) password authentication, to encrypted, highly secure smart card authentication.
- Network control protocols (NCP)
  NCPs are used to establish and configure different network protocol settings for IP, IPX, and NetBEUI. This negotiation includes negotiating protocol header compression and compression control protocol.

The resulting connection remains active until the line is disconnected for any of the following reasons:

- The user explicitly hangs up the line.
- The line drops due to idle time-out.
- The administrator hangs up the line.
- An unrecoverable link error occurs.

Link Control Protocols

Link Control Protocols (LCP) establish and configure PPP framing. PPP framing defines how data is encapsulated before transmission on the wide area network. The PPP standard framing format ensures any vendors' remote access software can communicate and recognize data packets from any remote access software that adheres to the PPP standards. PPP and Windows 2000 use variants of High-level Data Link Control (HDLC) framing for serial or ISDN connections.

Authentication protocols

Negotiation of authentication protocols occurs immediately after link quality determination and before network layer negotiation. For more information about available authentication protocols, see Authentication.

Network control protocols

Network control protocols establish and configure different network protocol settings for TCP/IP, IPX, NetBEUI, and AppleTalk. The following table describes network control protocols used with a PPP connection.

Network control protocol	Description
Internet Protocol Control Protocol (IPC)	IPC is used to configure, enable, and disable IP modules at both ends of the connection. IPXCP is used to configure, enable, and disable IPX modules at both ends of the connection. IPXCP is widely implemented by vendors.
Internet Packet Exchange Control Protocol (IPXCP)	The IPX WAN protocol is Novell's alternative to IPXCP. IPX WAN is not compatible with IPXCP. Windows 2000 supports IPXCP, which is implemented by the vast majority of remote access software.
NetBEUI Control Protocol (NBTP)	NBTP is used to configure, enable, and disable NetBEUI protocol modules at both ends of the connection.
AppleTalk Control Protocol (ATCP)	ATCP is used to configure, enable, and disable the AppleTalk protocol modules at both ends of the connection.

4.1.1 PPP RFC's

Requests for Comments (RFC's) are an evolving series of technical reports, proposals for protocols, and protocol standards used by the Internet community. Routing standards are defined in RFC's published by the Internet Engineering Task Force (IETF) and other working groups. For information about configuring PPP settings in connections, see PPP settings. The following table lists the PPP RFC's.

RFC number	Title
1549	PPP in HDLC Framing
1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
1334	PPP Authentication Protocols
1332	The PPP Internet Protocol Control Protocol (IPCP)
1661	Link Control Protocol (LCP)
1990	PPP Multilink Protocol
2125	The PPP Bandwidth Allocation Protocol (BAP), The PPP Bandwidth Allocation Control Protocol (BACP)
2097	The PPP NetBIOS Frames Control Protocol (NBFCP)
1962	The PPP Compression Control Protocol (CCP)
1570	PPP LCP Extensions
2284	PPP Extensible Authentication Protocol (EAP)

Obtaining RFC's

You can obtain RFC's from the Request for Comments Web site. (http://www.rfc-editor.org/) This Web site is currently maintained by members of the Information Sciences Institute (ISI) who publish a classified listing of all RFC's. RFC's are classified as one of the following: approved Internet standards, proposed Internet standards (circulated in draft form for review), Internet best practices, or For Your Information (FYI) documents.

4.2 Windows 95/98 & Macintosh Multi-Link Configuration

CADVision's Help Section - Getting Connected Home <http://help.cadvision.com/> | Up <connect.asp>
Multilink PPP Setup Guide*Last updated: Sep 11, 2000*

This guide discusses how to set up multilink PPP (line binding) with a Windows 95/98 or Macintosh computer.
Click here to jump to the Windows 95 guide
Click here to jump to the Windows 98 guide
Click here to jump to the Macintosh guide (System 7.1 - 7.5.5)
Click here to jump to the Macintosh guide (Mac OS 7.6 or newer)

What is Line Binding?
Multilink PPP allows you to use two or more modem connections at the same time to increase your speed. With multiple 56k modems and multiple phone lines, you can connect at speeds up to 224 Kbps.
One of the most popular Multilink PPP systems is "Shotgun", a technology from Diamond Multimedia. Shotgun offers the high speeds of regular MPPP plus unique features such as manual control (add or release the second phone line on the fly), bandwidth-on-demand (auto-senses when you need greater bandwidth and automatically add the second phone line) and voice priority (the modem will auto-detect an incoming call and release the appropriate phone line to allow the call to come through -- this requires Telus' Call Waiting service and a Shotgun modem). Shotgun technology is available for Windows 95 and 98. As yet there has been no announcement of possible future availability of Shotgun technology for Macintosh.

Multilink PPP, however, is possible using the built-in Dial-Up Networking software in Windows 98, and is also possible with Windows 95 by installing the free Dial-Up Networking 1.3 upgrade. Macintosh computers with Mac OS System 7.1 or newer can bind up to two lines using FCR's LinkUPPP! Turbo dialler.

4.2.1 Setting up Multilink PPP on Windows 95

Windows 95 does not come with built-in support for multilink PPP. You need to install Microsoft's Dial-Up Networking Upgrade 1.3 to add this feature to Windows 95. You can obtain this software from Microsoft's website by following this procedure:

Open your web browser (Internet Explorer or Netscape Navigator/Communicator)
Visit the Microsoft website by typing the following URL into the Location or Address bar near the top of your screen, then pressing Enter:
http://www.microsoft.com
Internet Explorer users: click "Free Downloads" or point at "All Products" and click on "Downloads". Netscape users: click the "Downloads" link near the top of the page)
On the next page, select the following options and click "Find It"

- Product Name: All Products
- Operating System: Windows 95
- Show Me: All, by name

Scroll down and click on the "Dial-Up Networking Performance & Security Upgrade" link
Click the "Download Now" link on the next page
The next page will ask you to enter your e-mail address to verify if you have registered at Microsoft's site before; do so and click Continue
If you have not yet set up a profile at Microsoft's site, you will need to do so by following the prompts. If your profile does exist, enter your password, then click Next; you may be prompted to enter additional profile information; please do so by following the prompts.
Make sure the "Accept License Agreement and Download" option is selected, then click "Download Now"
Select the appropriate language for your version of Windows 95, then click Next

Click the "Download Now" button on the next page; you will be prompted to select a location to save the file; do so, then click Save and wait for the file to download

After downloading the file, open Windows Explorer (usually found in the Start menu under Programs); if you have a Windows key on your keyboard, you may also hold down this key and press "E" to bring up Windows Explorer

Locate the file you downloaded, and double-click it to begin installation of the Dial-Up Networking 1.3 Upgrade. After installing the upgrade, you will be asked to restart; do so, then follow the instructions in the Setting up Multilink PPP on Windows 98 section

4.2.2 Setting up Multilink PPP on Windows 98

The following instructions should also be used by Windows 95 users after performing the Dial-Up Networking 1.3 Upgrade as described above.

Double-click My Computer

Double-click Dial-Up Networking

Double-click "Make New Connection"

Name this connection "CADVision Multilink", then click Next

Enter the phone number 777-1336, the area code 403 and the country code Canada (1), then click Next

Click Finish

A new "CADVision Multilink" icon will appear; click it ONCE with your RIGHT mouse button and select properties

In the General tab, ensure that "Use area code and Dialing Properties" is NOT checked. Ensure that your correct modem is selected here.

Click on the Server Types tab. Ensure that ONLY Enable software compression and TCP/IP are checked (NOTE: If you use Microsoft FrontPage, you will also need to check Log on to network)

Click on the Multilink tab, and select "Use additional devices"

Click the Add button; select a modem from the list (NOT the same one you have selected in the General tab). The phone number should be 777-1336.

If you have a 3 or 4 line Multilink PPP account with CADVision, you may add a third and fourth modem in this list as well, all with the phone number 777-1336.

Click OK to save your changes. You are now ready to connect by double-clicking the CADVision Multilink icon

4.2.3 Setting up Multilink PPP on a Macintosh (System 7.1 - 7.5.5)

Multilink PPP on a Macintosh can be achieved using special dialling software in conjunction with either the MacTCP ("Classic Networking") or Open Transport networking software. Open Transport is much more stable, flexible and powerful, so it is the recommended choice if you have at least 16 MB of RAM. You can install Open Transport 1.1.1 or newer on your system using the following procedure (which in turn requires at least System 7.1). You will need a copy of the CADVision Connection CD version 2.0.

Insert the CADVision CD into your CD-ROM drive

If the Installer window opens, click Quit

Double-click the "CADVIS2" CD icon on your desktop

Scroll down until you see the Open Transport 1.1.1 Install folder, then double-click it

Double-click the Installer icon, then click the Continue button when it appears

Click Install, then click the "Restart" button when it appears

Follow the instructions in the Setting up Multilink PPP on a Macintosh (Mac OS 7.6 - 8.6) section

Setting up Multilink PPP on a Macintosh (Mac OS 7.6 or newer)

Before you can establish a Line Binding connection on your Macintosh, you will need to obtain a multilink PPP dialler such as FCR Software's LinkUPPP! Turbo (which is what we will discuss here). At the time this document was written, the latest version of LinkUPPP! Turbo is 3.0, available for $59.95 (USD) from FCR's website

(http://www.fcr.com). A free 30-day trial copy is also available. Use the following procedure to download the trial copy.

Downloading LinkUPPP! Turbo 3.0

Open your web browser (Netscape or Internet Explorer) and enter the following URL in the Address or Location bar:

http://www.fcr.com

Click "Products", then, on the next page, click "LinkUPPP! Turbo 3.0"

To download the trial copy of the software, click "Try It!"

You will need to enter some information about yourself here; do so then click "Submit"

Click the "Download Here" link to begin the download. You will be prompted to select a location to save the file; select a location (the desktop is a good choice), then click "Save"

After downloading the software, you will have a file with one of the following names: "LinkUPPP_Turbo_3.0.3.hqx", "LinkUPPP! Turbo Installer.sea" or "LinkUPPP! Turbo Installer". Follow the appropriate instructions for the file you have:

- If you have the file whose name ends in ".hqx", drag it onto your StuffIt Expander application (StuffIt Expander is included with every version of Netscape Navigator or Communicator beginning with version 4.0, and on every Macintosh with Mac OS 8.0 or later. If you need it, you can get a copy of StuffIt Expander from the CADVision Macintosh Toolkit version 2.0). You should be asked where you'd like to save the expanded file; select a location, then click "Expand". Skip to the next section.
- If you have the file whose name ends in ".sea", simply double-click it and it will expand itself. You will be prompted where you would like to save the expanded file; select a location and then click "Expand" or "Save". Skip to the next section.

If you have the "LinkUPPP! Turbo Installer" file, skip to the next section

Installing LinkUPPP! Turbo 3.0

Double-click the "LinkUPPP! Turbo Installer" icon to begin installing the LinkUPPP! Turbo 3.0 dialler software.

Click "Continue" when the title screen appears

Click "Accept" on the License Agreement

The LinkUPPP! Turbo instructions screen will appear; you can print these if you wish by clicking the "Print" button, or simply click "Continue"

Click "Install"

After the installation is complete, you will be given the option to "Continue", "Quit" or "Restart"; click "Restart" to restart your computer so you can use the new software

Configuring the TCP/IP control panel

If you are using Open Transport, you will have a control panel called "TCP/IP" - you need to ensure the TCP/IP control panel is set up correctly before you can use LinkUPPP! Turbo.

Under the Apple menu, select Control Panels --> TCP/IP

Next to "Connect via:" select "TCP/IP PPP" (not "PPP")

Next to "Configure using:" select "PPP Server"

Enter the following two addresses under "Name Server Addr.":

- 207.228.64.43
- 207.228.64.5

Enter the following domain name under "Additional Search Domains":

cadvision.com

Close the TCP/IP control panel; click "Save" to save your changes when prompted

Make sure AppleTalk is not using one of your serial ports

AppleTalk is a different networking scheme that is used to connect Macintosh computers and printers. If AppleTalk is enabled, it may be set to connect using your Printer Port or Modem Port, which will prevent you from being able to use that port for a modem. Please follow these steps to ensure that AppleTalk is not using one of your serial ports:

Under the Apple menu, select Control Panels --> AppleTalk

If you are prompted with a message that says AppleTalk is currently inactive, click "No" and immediately close the AppleTalk control panel, then skip to the next section

Ensure that you do NOT have your Modem or Printer port selected next to "Connect via:"; it is not a problem if you have Ethernet or IRDA or something else selected here

Close the AppleTalk control panel; click "Save" to save your changes if prompted

If you have any problems getting connected, you might also want to open the "Chooser" (from the Apple menu) to make sure you do not have AppleTalk enabled or using one of your serial ports.

Configuring LinkUPPP! Turbo 3.0

Open the LinkUPPP! Turbo application

Enter the following information:

- Phone Number: 777-1336
- Username: (your login ID)
- Password: (your password)

Check "Save Password" to avoid having to type in your password every time you connect; uncheck "Modem Speaker" if you don't want to hear the modems making noise while connecting

Click on the small triangle next to "Dial-up Options" to open that section

Uncheck "Prompt for Username and Password"

Click on the triangle next to "Dial-up Options" again to close that section

Click on the triangle next to "Expert Settings" to open that section

Uncheck "CHAP" under "Enable Authentication"

Check "Enable Turbo (Dual Modem) Mode"

Check "Enable VJ Compression" under "Enable IPCP Negotiation"

Uncheck "Enable ATCP Negotiation"

Click on the triangle next to "Expert Settings" to close that section

Next to "Modem 1", select your modem type (if it's not listed here, see the section below entitled "Installing New LinkUPPP! Turbo Modem Scripts"), and next to "Port 1" select the serial port to which your first modem is connected (Printer Port, Modem Port, or Internal Modem; there may be other options here as well)

Next to "Modem 2" and "Port 2" select your second modem type and port, same as above

Set the number of Links to "2" or "Auto" (the latter choice will automatically add the second connection when it detects that you need more bandwidth, whereas choosing "2" will cause both modems to dial in one after the other to establish 2 links right away)

Choose "Quit" from the "File" menu to close the program; save your changes as "CADVision" when prompted

4.3 Multi-Link configuration for Windows 2000.

4.3.1 Enabling Multiple devices

To enable multiple device dialing
Open Network and Dial-up Connections.

1. Right-click the connection on which you want to enable the dialing of multiple devices, and then click **Properties**.
2. On the **Options** tab, in **Multiple devices**, do one of the following:
   - If you want Windows 2000 to dial only the first available device, click **Dial only first available device**.
   - If you want Windows 2000 to use all of your devices, click **Dial all devices**.
   - If you want Windows 2000 to dynamically dial and hang up devices as needed, click **Dial devices only as needed**, and then click **Configure**.

     In **Automatic dialing**, click the **Activity at least** percentage and **Duration at least** time you want to set. Another line is dialed when connection activity reaches this level for the amount of time that you specify.

     In **Automatic hangup**, click the **Activity no more than** percentage and **Duration at least** time you want to set. A device is hung up when connection activity decreases to this level for at least the amount of time that you specify.

Notes

- To open Network and Dial-up Connections, click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**.
- If you selected **Dial devices only as needed**, the last multilinked device ignores the **Automatic hangup** setting, and a twenty-minute time-out is used for the last device.
- If you use multiple devices to dial a server that requires callback, then only one of your multilinked devices is called back. This is because only one number is stored in a user account. Therefore, only one device connects and all other devices fail to complete the connection, and your connection loses Multilink functionality.
  You can avoid this problem if the multilinked phonebook entry is an ISDN with two channels that have the same phone number.
- Multiple device dialing is available only if multiple adapters are available on the computer.
- If you select **Dial all devices**, dropped links in the multilinked bundle are not automatically reinitialized. You can force links to reinitialize by selecting **Dial devices only as needed**, then **Configure**, and then setting easily achieved **Automatic dialing** conditions which cause another line to be dialed. For example, set **Activity at least** to 1% and **Duration at least** to 3 seconds.

4.3.2 Configuring multiple device dialing

The Network and Dial-up Connections feature performs PPP Multilink dialing over multiple ISDN, X.25, or modem lines. The feature combines multiple physical links into a logical bundle and the resulting aggregate link increases your connection bandwidth. To dial multiple devices, both your connection and your remote access server must have Multilink enabled.
Network and Dial-up Connections can dynamically control the use of multilinked lines. By allocating lines only as they are required, thereby eliminating excess bandwidth, you can realize a significant efficiency advantage. You can configure the conditions under which extra lines are dialed, and underused lines are hung up, through Network and Dial-up Connections settings.

For more information, see To configure multiple device dialing.
Note

- If you use Multilink to dial a server that requires callback, then only one of your multilinked devices is called back. This is because you can only store one number in a user account. Therefore, only one device connects and all other devices fail to complete the connection, and your connection loses Multilink functionality. You can avoid this problem:
    - If the multilinked phonebook entry uses an standard modem configuration, and the remote access server that your connection is calling uses more than one line for the same number.
    - If the multilinked phonebook entry is ISDN with two channels that have the same phone number.

4.4 Telnet Options and Commands

Table 126: telnet Command Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route *path*	Specifies loose source routing. The *path* argument is a list of host names or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running Unix-to-Unix Copy Program (UUCP) and other non-Telnet protocols.
Port-number	Port number.
Bgp	Border Gateway Protocol.
Chargen	Character generator.
cmd *rcmd*	Remote commands.
Daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Host name server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
node	Connect to a specific LAT node
pop2	Post Office Protocol v2.

pop3	Post Office Protocol v3.
port	Destination LAT port name.
smtp	Simple Mail Transport Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specify TACACS security.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	Unix-to-Unix Copy Program.
whois	Nickname.
www	World Wide Web.

With the Cisco IOS implementation of TCP/IP, you are not required to enter the connect or telnet commands to establish a terminal connection. You can just enter the learned host name—as long as the following conditions are met:

- The host name is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.
The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the host name, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.
The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is **Ctrl-^** (press and hold the **Ctrl** and **Shift** keys and the **6** key). You can enter the command character as you hold down **Ctrl** or with **Ctrl** released; you can use either uppercase or lowercase letters. Table 127 lists the special Telnet escape sequences.

Table 127: Special Telnet Escape Sequences

Escape Sequence	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

[1]The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

Ctrl-^ ?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the **Ctrl** key, while the second caret represents **Shift-6** on your keyboard:

```
router> ^^?
```

```
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch back and forth between them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.
To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples
The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to kl.sri.com, then to 10.1.0.11, and finally back to *host1*:

```
router> telnet host1 /route:kl.sri.com 10.1.0.11 host1
```

The following example connects to a host with logical **name *host1:***

```
router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router> telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is done using the optional **/quiet** keyword:

```
login:User2

Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout

    User2        logged out at  16-FEB-2000 09:38:27.85
```