Speed Your Protocol Design Cycle

Presented by Dave Whipple,

Lead technologist for cdma2000 and W-CDMA

Agilent Technologies

This presentation is part two of a series on test and simulation issues associated with protocols on the air link of wireless cellular systems. This paper includes a short review of the first paper, so if you haven't seen that, this presentation will still be of value.

Agenda

- Review of prior paper
- Generic wireless protocol model
- GPRS and cdma2000 layers and probes
- Ladder diagrams
- Logging examples
- Summary

Agilent Technologies

So much of the industry needs are independent of the radio format; this presentation will treat them as a group. Specific examples will be given from either cdma2000 or GPRS.

The presentations will review the first presentation, then move into details of the protocols used for packet data connections for both GPRS and cdma2000. A detailed example will be presented.

Problem Statement

- **Increased complexity of standards and devices**
- **Time to market pressure**
- **New features**
  - **Pictures**
  - **Browsing**
  - **Modem functions**

Agilent Technologies

The wireless industry has added numerous new features to the networks and the phones. One major element of this is the availability of packet switched data with its associated sharing of system resources. Despite the added complexity of design, there is much higher pressure on time-to-market now than in previous systems. This is due to the maturity of the industry and the customer base. Missing an introduction by a few months may cost millions in revenues.

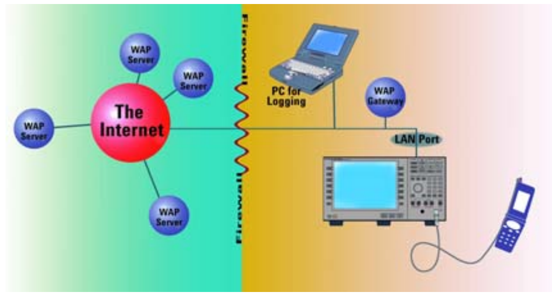
One note on the terminology of the wireless appliance. It may be a phone, a handset, a PDA, a PCMCIA modem – or some other form that may be yet to come. I will use the term wireless device, handset, or phone, in most cases. This is meant to apply to any wireless appliance, and not imply any particular implementation.

Three major challenges exist in the test environment:

1. Connection to the Internet
2. Emulate Real-World RF Environment
3. Monitor the Messages Over-the-Air

These will be further discussed in the following slides.

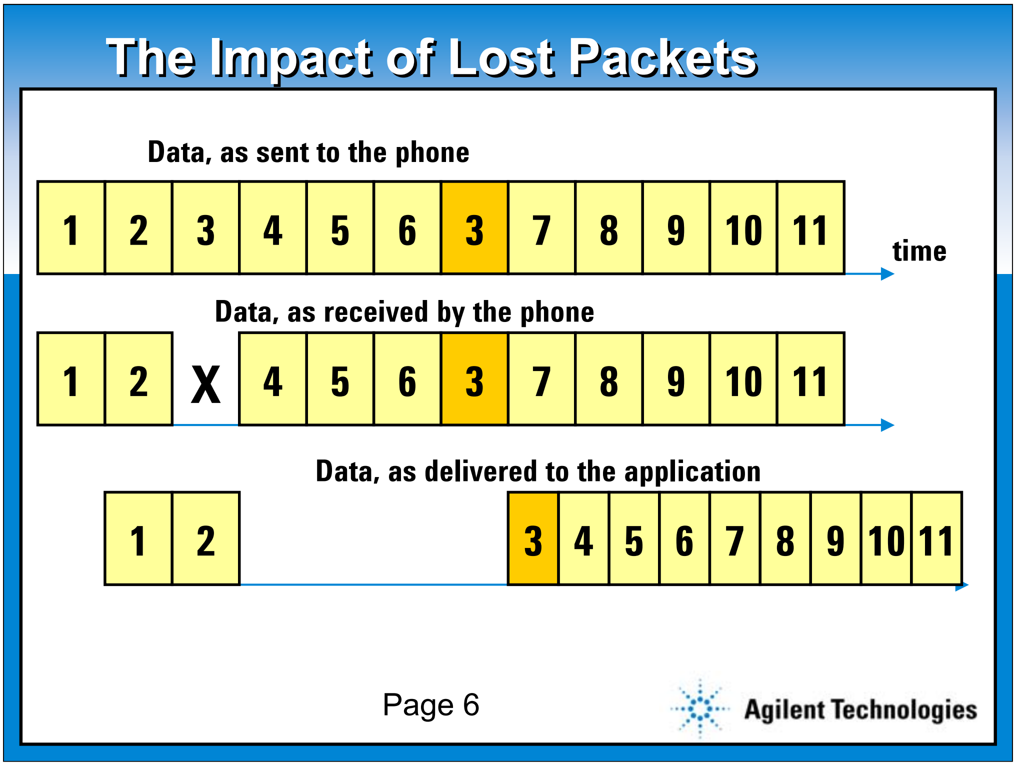
Put the Network on Your Bench



- **Access multiple technologies/networks in your work area in one instrument**
- **Affordable**
- **Easy to use**
- **High rate data connection**

Agilent Technologies

One solution is to put wireless access on your bench. The test products become the transducer between the Internet and the wireless device being developed or tested. Full message instrumentation is available for the link.

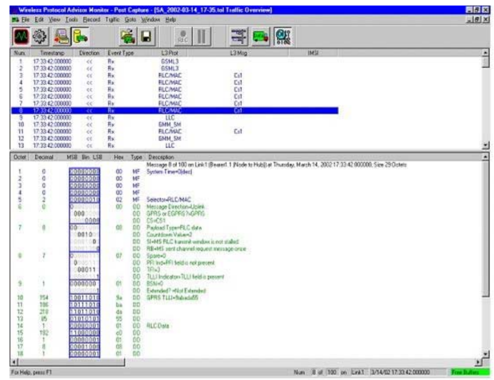


This picture shows the effect of a lost packet. Packet 3 is lost in its transmission. Not shown are the messages between the phone to the network asking for a re-transmission. The network is required to put higher priority on re-transmission of a lost packet than on the transmission of a new packet, so the lost packet is sent over the air quickly.

The network has memory requirements to keep a copy of each transmitted packet long enough to be sure a re-transmission won't be requested. The phone has memory requirements to buffer the packets received after the lost one, and build the data stream correctly after the lost packet is received correctly. As you can see here, the application does not get a steady flow of data, but may have gaps with no data at all.

The messages, priorities, and rules for memory management in both the network and the phone are all part of the standard, so the test environment must be uniquely modified for each standard.

Wireless Protocol Advisor

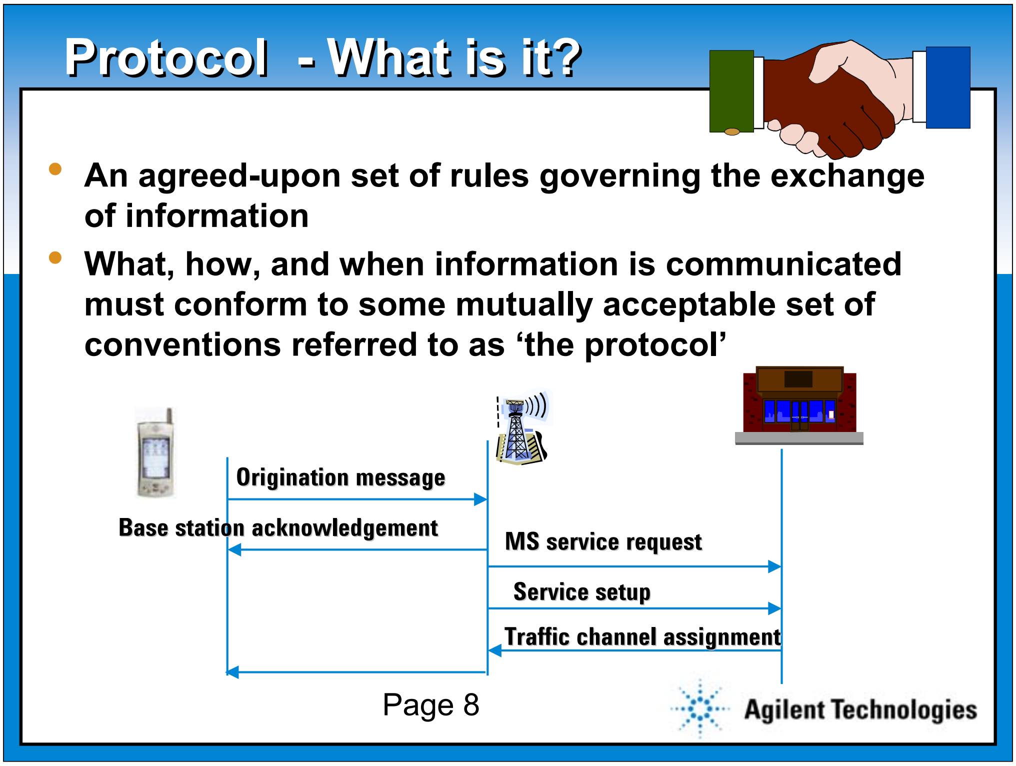


- Real-time logging
- Raw data analysis
- Filtering, triggering
- Post capture viewing
- Readable format – columnar, colors, Windows® -based
- Bi-directional messages

Agilent Technologies

Here is an example of a protocol log on the Agilent Wireless Protocol Advisor. The upper window is the sequence of messages, while the lower window provides the details of the message in blue in the upper window.

There is a breakdown in hex, decimal, and binary of the message, and the bit packing can be shown. The meaning of each field is shown green on the right.



In its simplest form, a protocol is a list of rules on what can be said, and when between network entities. The phone can only talk to a base station, but the base station has two underlying networks, the circuit switched phone network, and the packet switched data network, commonly called the Internet.

Certain message sequences will change the state of a phone. For instance, a phone may start in Idle state, and progress to a Voice state by sending an origination, and getting a channel assignment.

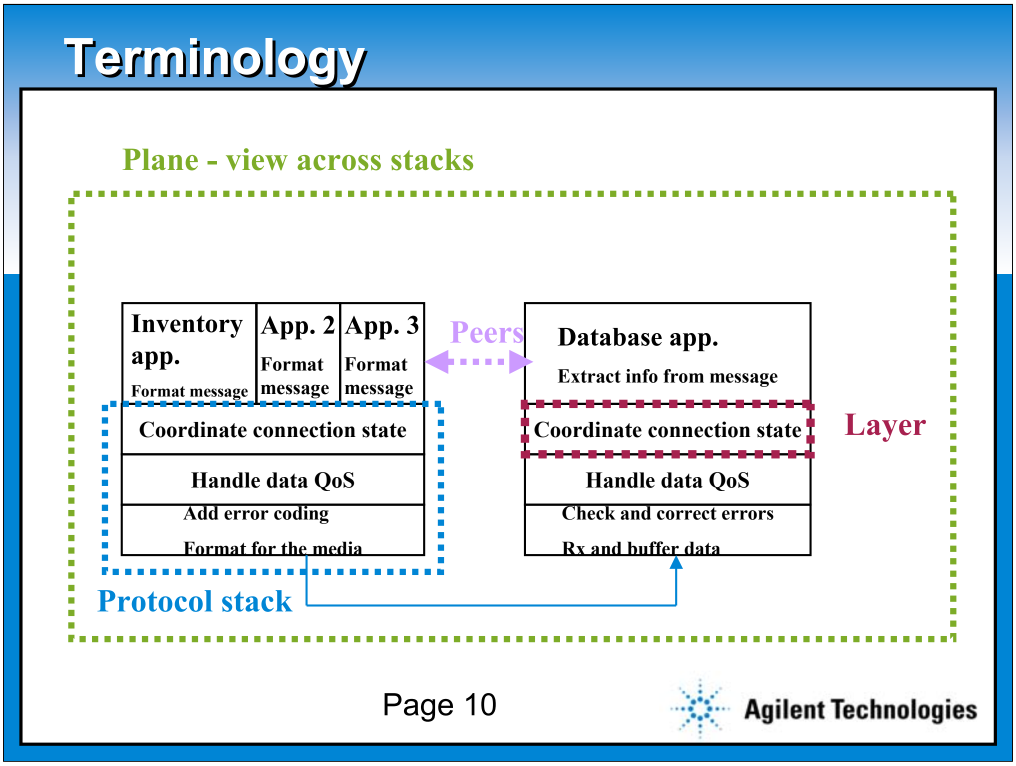
ISO-OSI 7 Layer Model

International Standards Organization - Open Systems Interconnection (ISO-OSI) 7 Layer Model		
Layer	**Function**	**Typical protocol**
Application	Specialized network functions such as file transfer, virtual terminal, electronic mail, and file servers.	
Presentation	Data formatting and character code conversion and data encryption.	
Session	Negotiation and establishment of a connection with another node.	
Transport	Provision for reliable end-to-end delivery of data.	TCP
Network	Routing of packets of information across multiple networks.	IP
Data Link	Transfer of addressable units of information, frames, and error checking.	MAC/RLC or RLP
Physical	Transmission of binary data over a communications network.	Physical Layer per Standard

Agilent Technologies

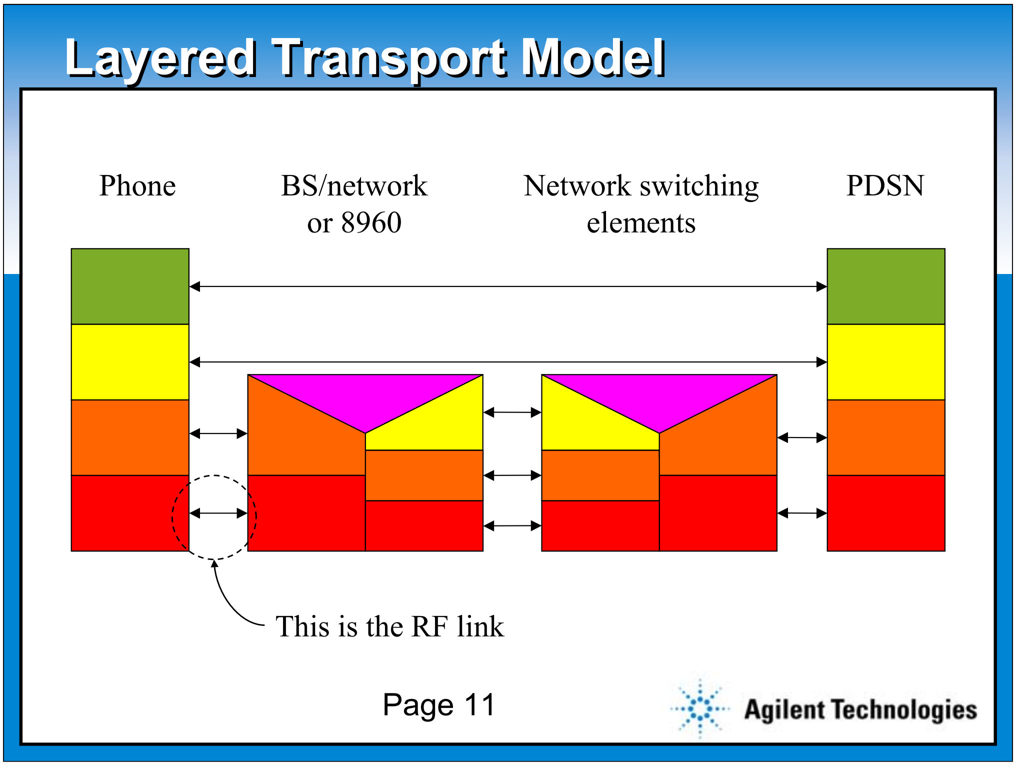
All of this layering is based on work done by the International Standards Organization in their Open Systems Interconnection 7 layer model. The physical link of GPRS does not have a unique name, it includes the coding, which can be to four different levels of error protection and the modulation. Layer 2 is comprised by the Radio Link Control (RLC) and another sub layer called the Medium Access Control (MAC). On the transmit side, these break apart a large data file into smaller packets suitable for transmission, and number each. On the Receive side, the RLC/MAC rebuilds the original large block. The higher layers are the same Internet Protocols we normally use in wired applications.

Most wireless systems violate the ISO-OSI model frequently. An example is the addition of a CRC on each data block. This is typically implemented in hardware; comprised of a shift register and a few XOR gates. As this is physical in nature, this is done as part of the physical layer, even though is specifically is a layer 2 operation in the model.



A view like this is called the plane view. It looks down on the layered structure, and shows the stack on each side. The stack is the collection of layers, and a layer is a single entity with specific role in the overall process.

Each layer in has two roles: transport messages to and from higher layers, and to exchange messages with its peer. A peer is always at the same layer on the opposite side of the link. So, while a message from an upper layer is transported down by each of the lower layers, transported by the physical layer to the bottom of the alternate stack, it rises up the stack and ends at the same layer as it started. Any layer cannot communicate with any layer on the other side other than its peer.

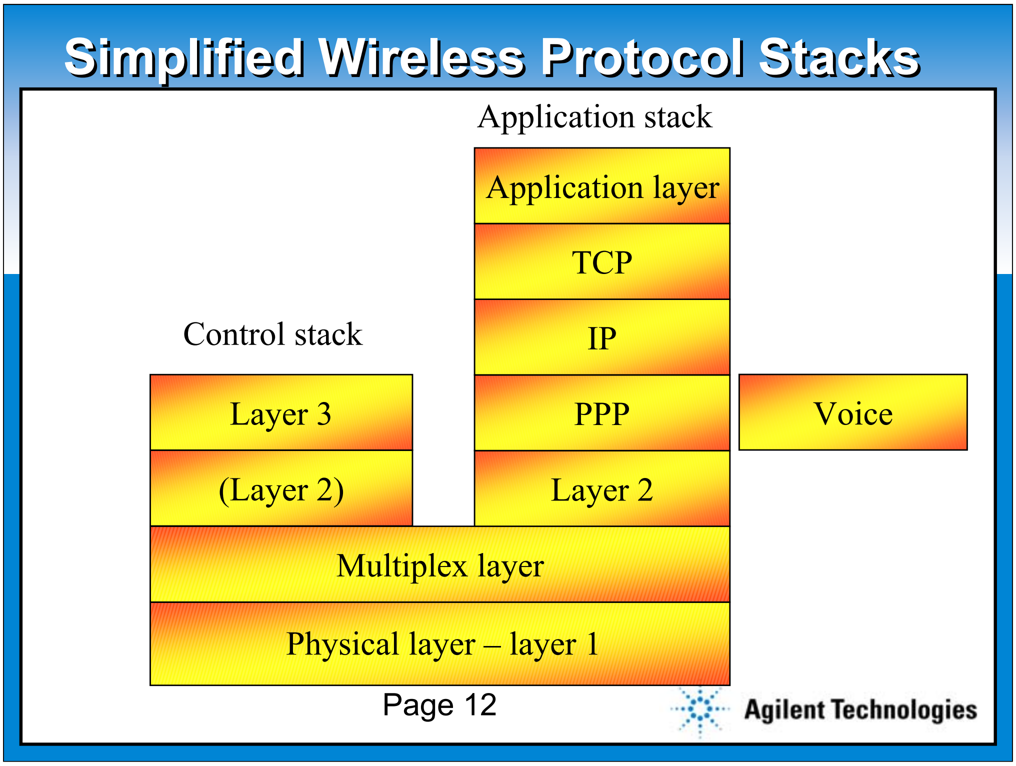


This shows how different layers of a stack can come from different devices. The stack on the left represents the phone, the second the base station, the network, and a mapping function needed to get the data to the Internet. The third stack represents other switching elements. The stack on the right is the Internet. The phone has physical and data flow connections with its own cell, but the next layer up, IP, is transferred from the internet. It has been passed through each of the intermediate pathways.

It should be noted that each layer in the phone has a peer, but that peer may reside at many locations throughout the network.

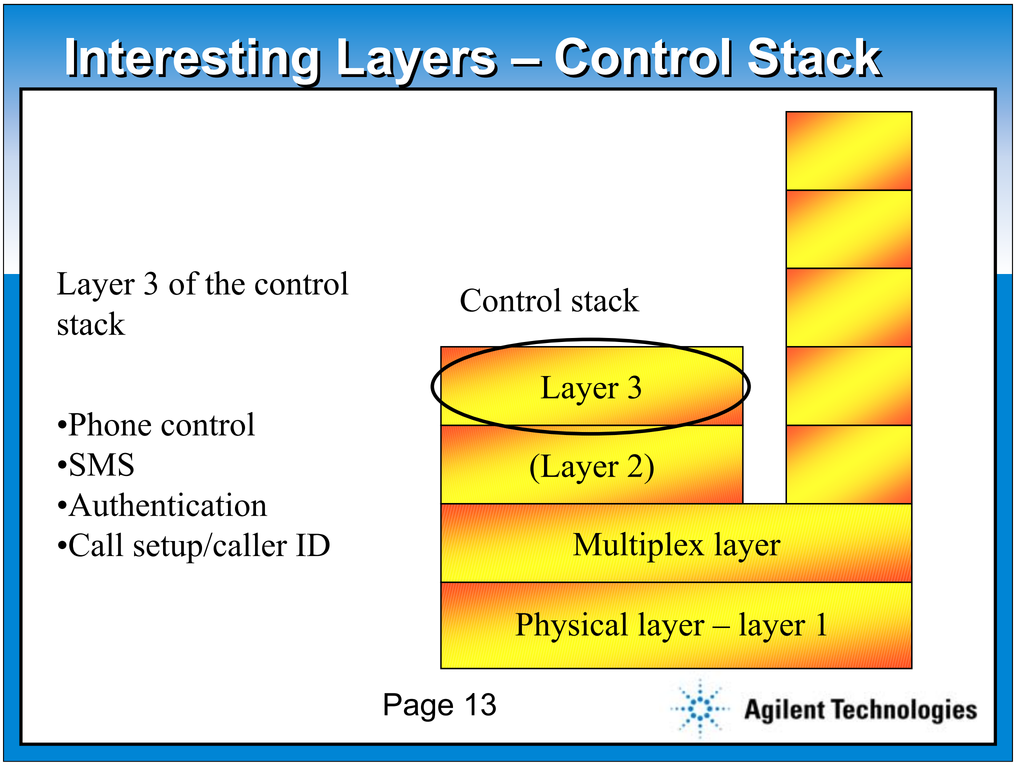
The black line with two arrows circled at the bottom left represents the RF link in both directions. We have spent a major part of our careers measuring power, noise, harmonics, sensitivity, spectral purity of this link.

Products that focus on the higher layers, while similar to those designed to test the RF link, focus on the messages and Internet content, rather than on RF parametric tests.



This is a simplified set of stacks. There are really two stacks active when in a packet session. These are the control stack and the application stack.

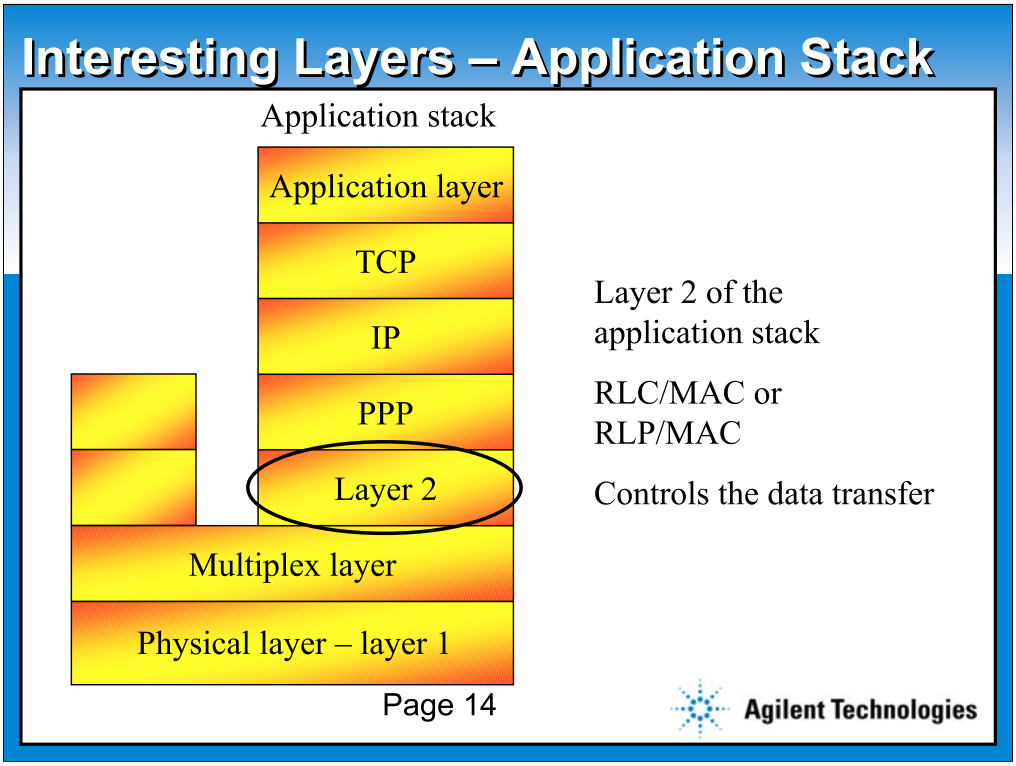
If the desired service were voice, it would lay on top of layer 2 of the application stack, with no higher layers. Layer 2 in this case is not very active.



The control stack is where the phone control happens. It is active whether a phone is active or inactive. It may be carried on numerous different physical layers. Typically, there are control channels for this when inactive, and the messages may compete for the traffic channel when active. In modern systems such as cdma2000 and W-CDMA, there may be dedicated channels in parallel to the application. Most of the interest in at layer 3.

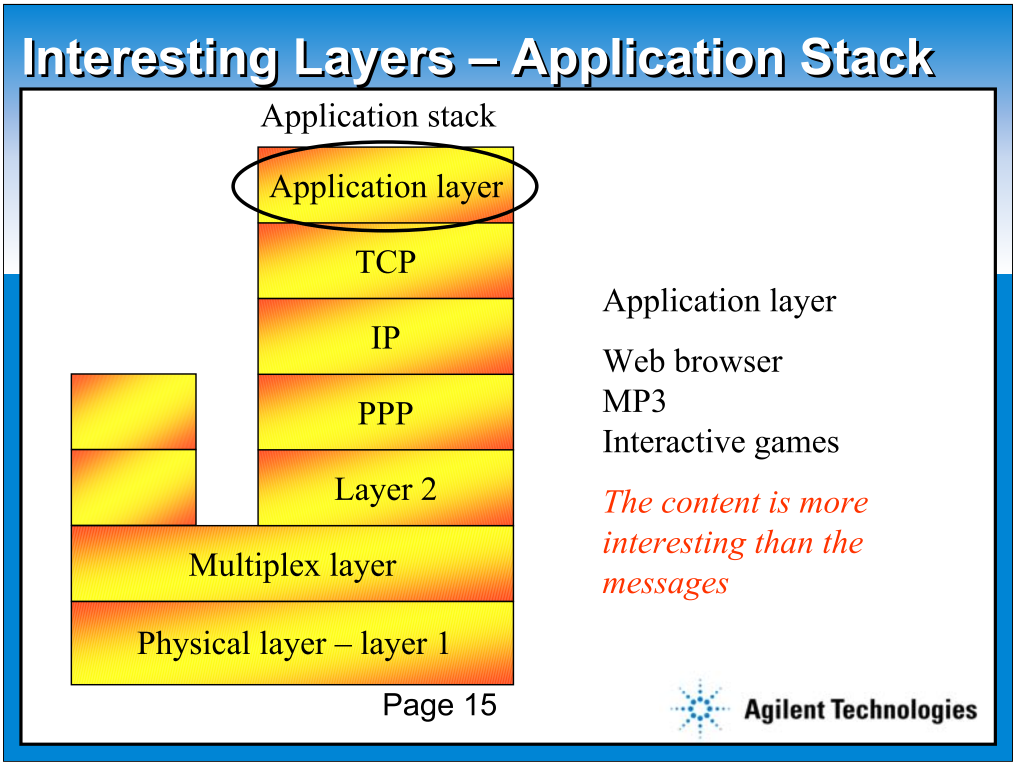
In general, the control stack is not used for functions that generate any revenue to the network operator. One exception to this is Short Message Service (SMS). These short messages are often carried on the control channels.

Layer 2 exists for the control stack, but typically doesn't have too many messages. A typical rule for layer 2 would be to force re-transmission of a layer 3 message if it was not acknowledged within 300 msec of the original transmission by the receiving end.



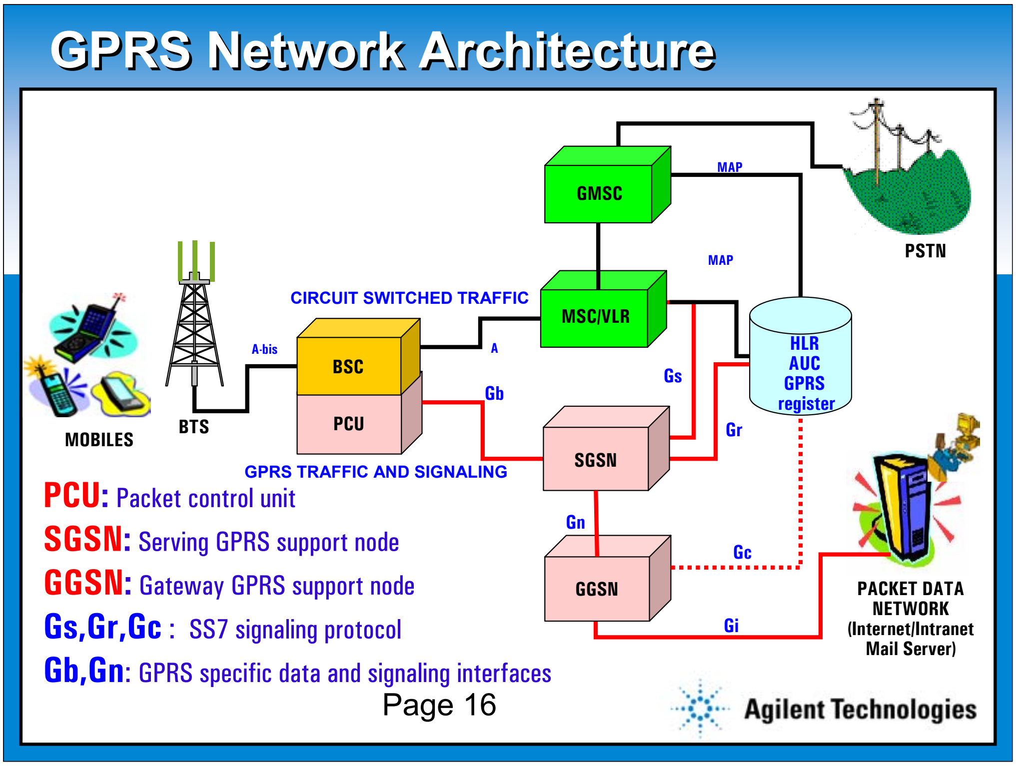
The application stack may take many forms, depending on the nature of the service. Shown here would be Internet access. If a file transfer was started using FTP, the stack would be quite different.

This model fits cdma2000 reasonably well, but is not very accurate for GPRS or W-CDMA.



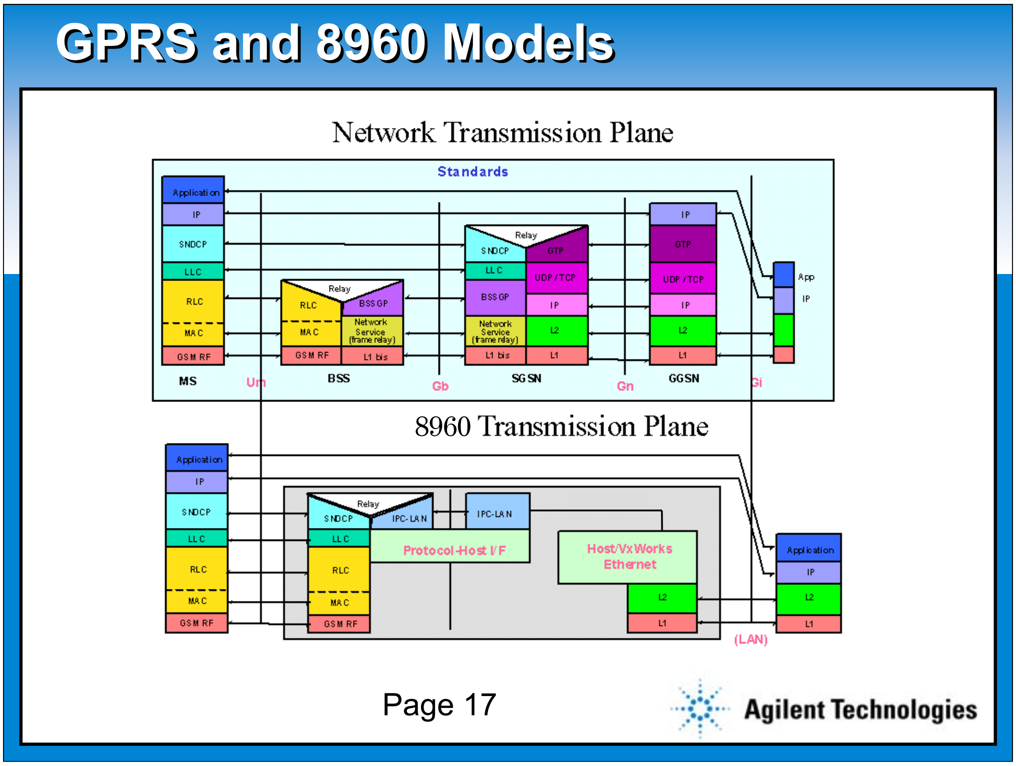
The application layer is the destination for the content from the Internet. The messages controlling the flow of data have all occurred at lower layers, and the content is delivered.

It is at this layer that the RF effects of re-transmitted packets are evaluated.



The GPRS network brings in many changes to the existing network. In fact most of the changes are amendments with new blocks rather then modifications of existing resources. The data traffic and signaling is controlled by two new blocks: the GGSN and SGSN. The subscriber database is still managed by the VLR and HLR, hence we need signaling links between the these Service Nodes to the HLR and VLR. Since GPRS is a packet switched network and GSM until now was circuit switched, this brings is some changes to the air interface structure. As a result changes are required in managing the packet transfer over the air interface. This is a done by a piece of additional software block in the BSS which is the PCU (packet control unit).

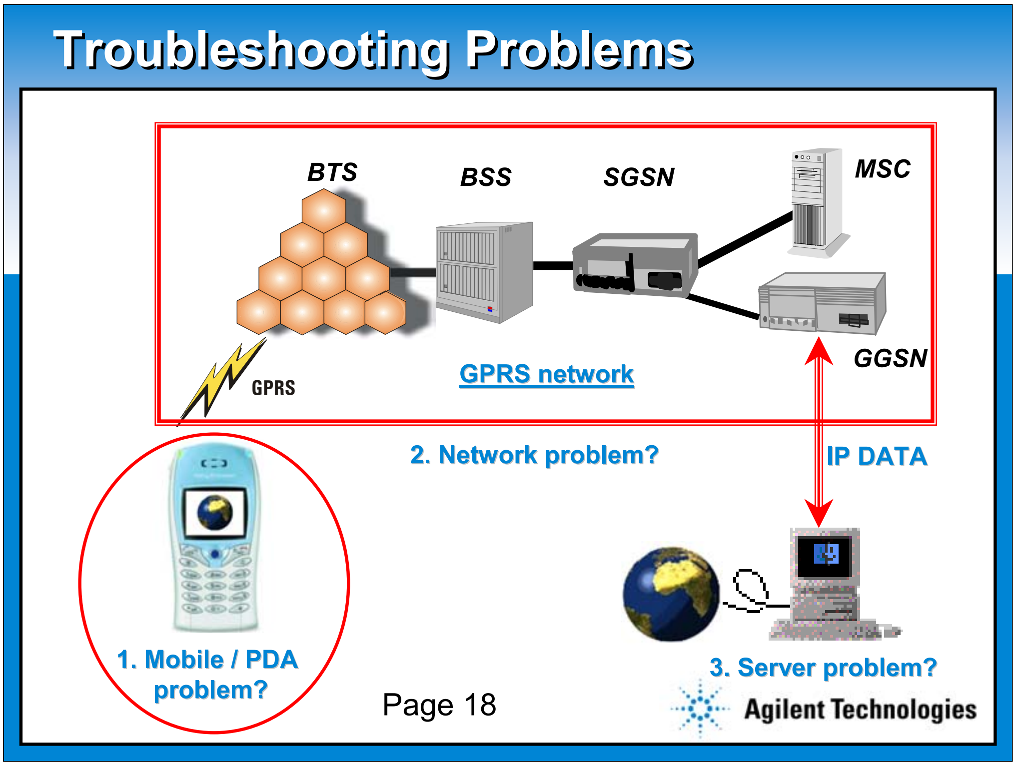
The signaling links between the GPRS nodes and the GSM blocks will be SS7 MAP interfaces. The signaling between GPRS nodes with follow the GPRS protocol stacks as defined by the specifications.



The top picture shows the actual protocol stacks for the data portion of GPRS. On the left is the phone, next is the cell, then the switch, followed by a special switching network to get to the Internet. Finally, on the right, is the Internet itself.

On the bottom is a representation of what is inside the 8960 with the GPRS Lab Application. All of the network elements have been realized in one stack, and the layers starting at IP and going higher have been reflected to the network port on the 8960. This is an Ethernet connection, with its own physical and data link layers, while the IP and higher layers are passed through to the phone, just as in a real network.

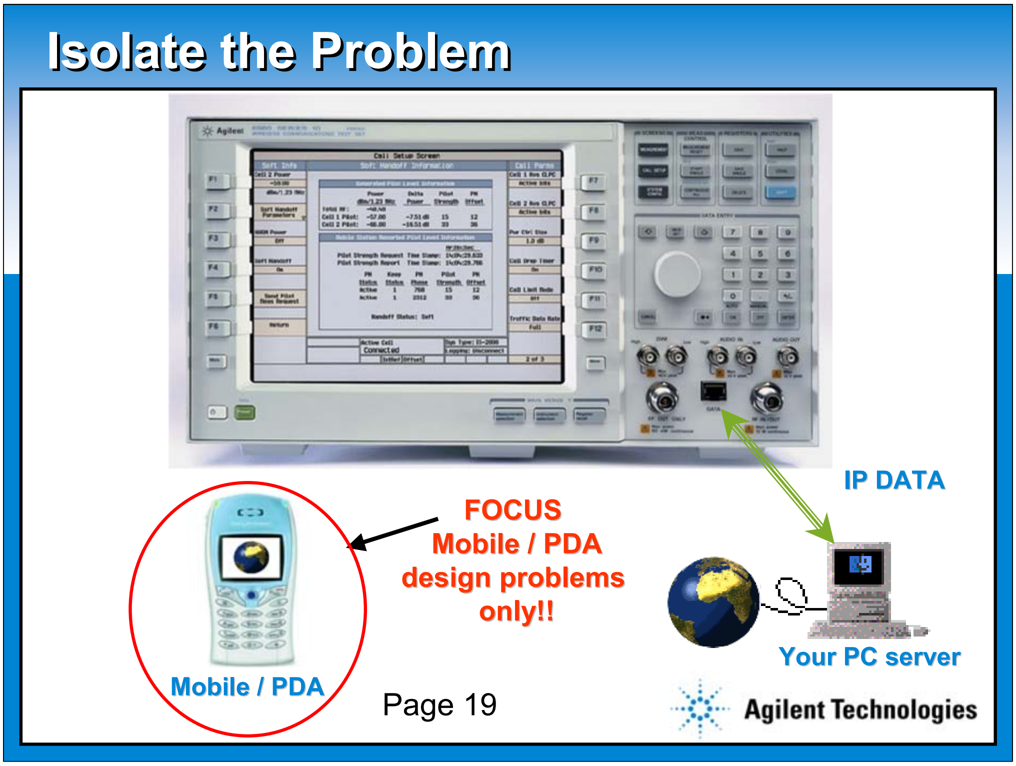
.



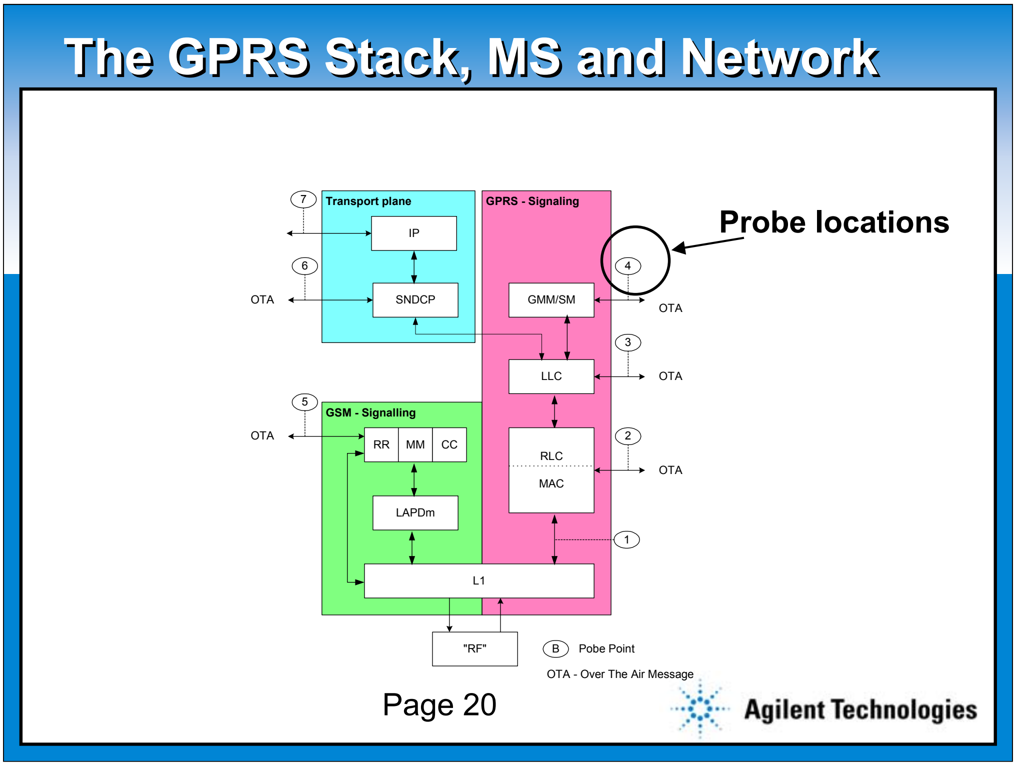
When you evaluate a phone design, it may be very difficult to find out the data transmission problems.

The problems may come from the network components, computer server, or the mobile phone.

Mobile phone R&D engineers would like to evaluate whether their products work properly under real data transmission.

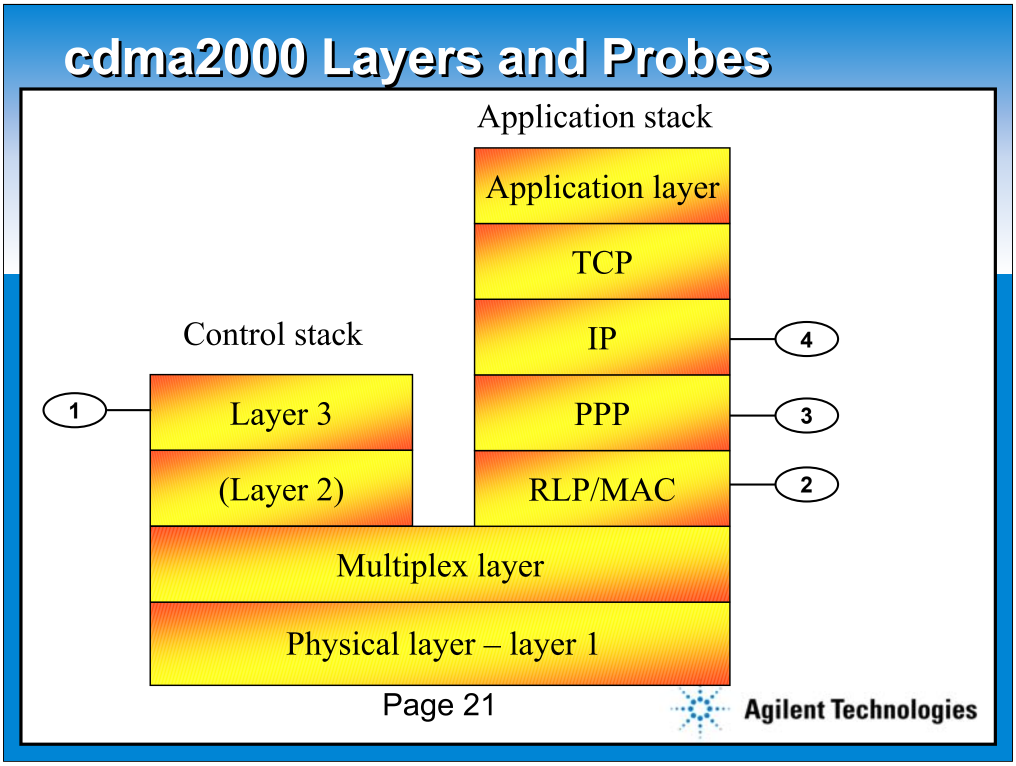


The improved environment is to eliminate all the external switching elements and the Internet. By using local network and Internet emulation, problems can be isolated just to the link to the phone and its internal protocol and application implementation.

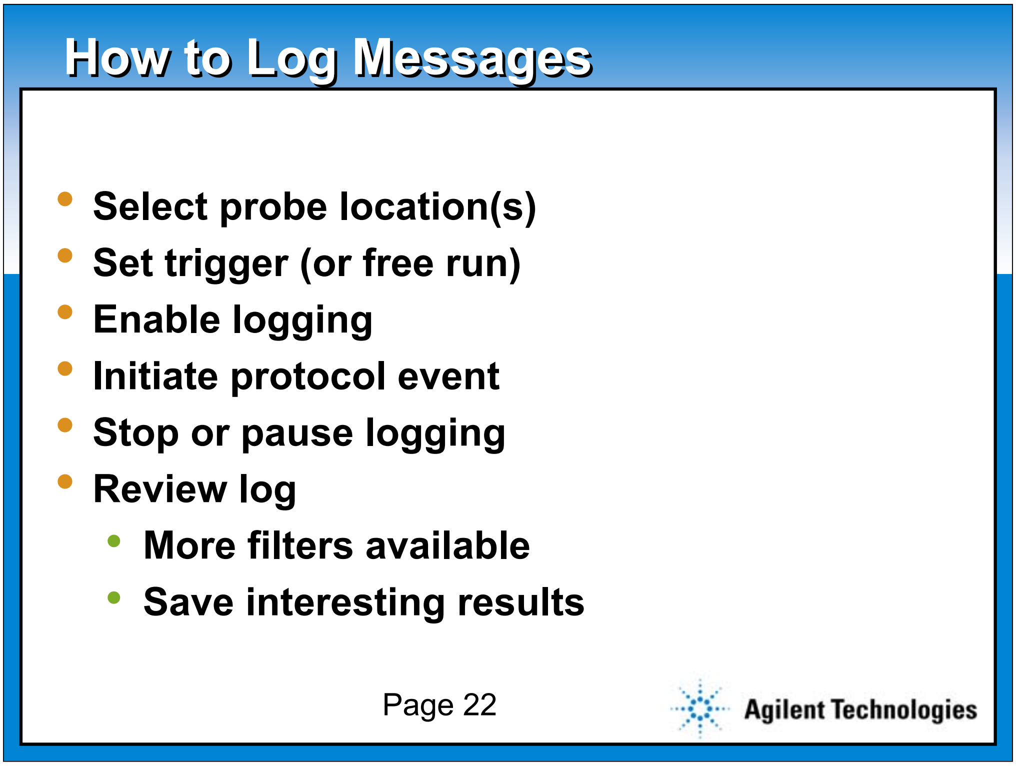


This is a more accurate view of the GPRS protocol stack. Since the layering is symmetrical, this could be either the base station/network, or the handset. In this case, three stacks are shown. The green block is the GSM transmission plane, the pink is the control plane, and the blue is the GPRS transmission plane. Note that the lower layers of the GPRS transmission are handled by the control plane.

The bubbles with numbers inside correspond to probe locations in the protocol logger.



This is very similar to the cdma2000 stack, and the probe locations are shown. As in GPRS, there are probes at layer 3 of the control stack, layer 2 of the application stack, and probes at a few higher layers.



The process of monitoring messages is discussed here. The steps are as follows:

Enable the probe(s) at each location of interest. Turning on too many probes simultaneously will be harder to analyze due to the amount of data collected.

Set up triggers. These can be on a specific message, for example. These can be used to eliminate the logging for the front end of a session and to get the data near the event of interest.

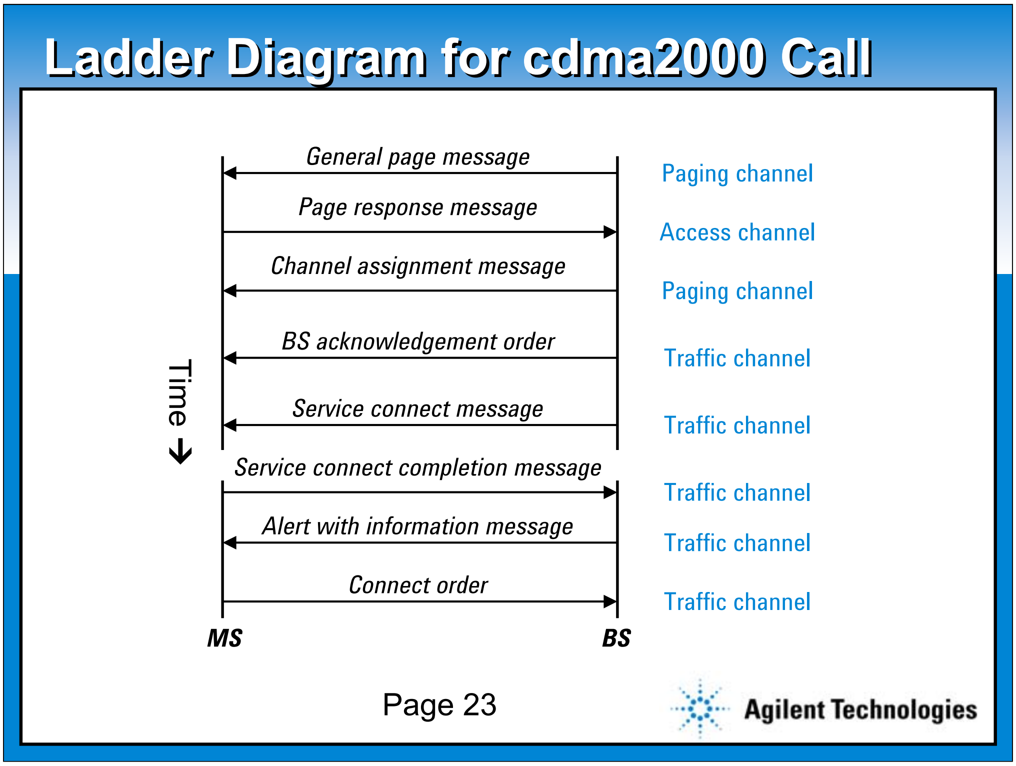
Enable logging. This starts reading the messages from the active probes, and will check against the trigger. Once started, the messages form a time stamped list.

Initiate the protocol event. This can be from the network end or the phone end.

Stop or pause the logging. After the events of interest, the log has been generated, and is in local memory of the protocol advisor.

Review the log. Additional filters are available to reduce the data being presented, if desired.

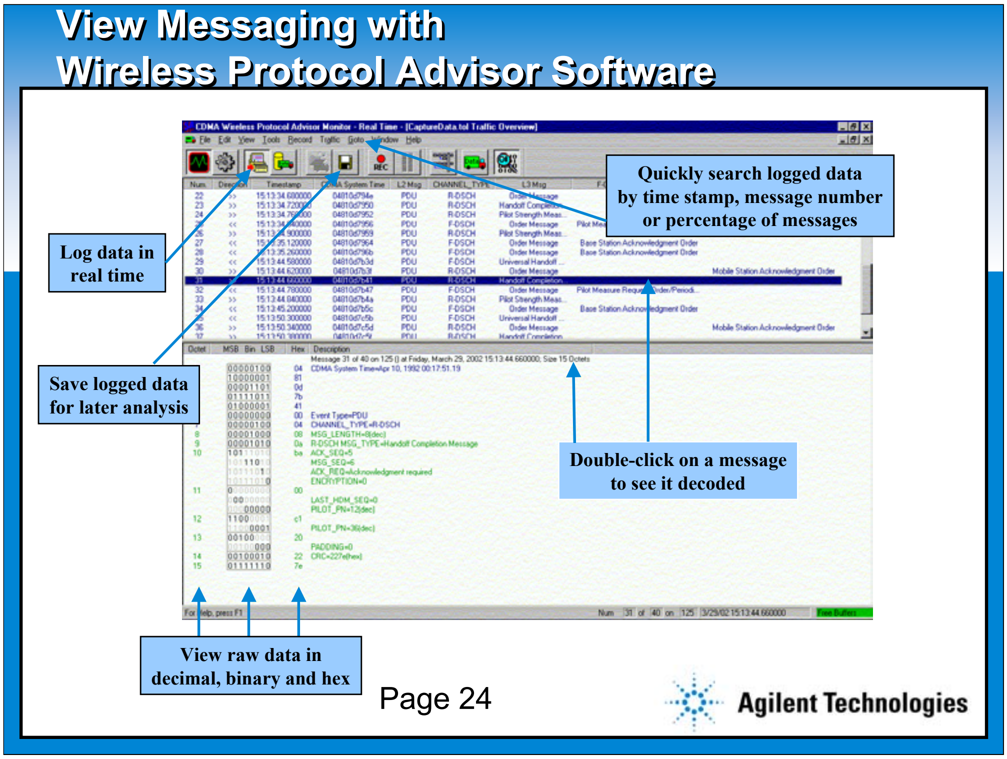
Save interesting results. This could be used for a bug report, for instance.



This call processing ladder diagram is from an Annex in the cdma2000 standard. It shows the messages needed for a network initiated voice call.

All of these messages are from layer 3 of the control stack. About 1/3 of the way through the log, the physical layer has been moved from the control channels to the traffic channels.

Time is running down the page, and the direction of the messages are shown with the arrows representing each message.



The E6910A's powerful and full-featured protocol analysis capabilities are provided by the Windows executable Wireless Protocol Advisor software running on an external PC, connected to the instrument via the LAN port. Includes:

•real-time logging of inter-layer and peer-to-peer messages

•IP datagram capture and display

•traffic overview summarizing logged message information

•decode view for viewing individual bit fields with appropriate labeling for each message

•raw data in decimal, binary and hex

•data can be saved

•data can be searched

Message Log from 8960

	Num.	System Time	Channel Type	Event Type	L3 Msg	ORDER
*	1	07:29.68	f-csch (F-PCH)	PDU	General Page Message	
	2	07:30.32	r-csch	PDU	Page Response Message	
	3	07:30.48	f-csch (F-PCH)	PDU	Extended Channel Assignment Message	
	4	07:30.98	f-dsch	PDU	Order Message	Base Station Acknowledgment Order
	5	07:31.02	f-dsch	PDU	Order Message	Pilot Measure Request Order
	6	07:31.06	f-dsch	PDU	Service Connect Message	
	7	07:31.06	r-dsch	PDU	Pilot Strength Measurement Message	
	8	07:31.12	r-dsch	PDU	Order Message	Mobile Station Acknowledgment Order
	9	07:31.22	r-dsch	PDU	Service Connect Completion Message	
	10	07:31.32	f-dsch	PDU	Alert With Information Message	
	11	07:31.42	r-dsch	PDU	Order Message	Mobile Station Acknowledgment Order
	12	07:31.58	f-dsch	PDU	Order Message	Base Station Acknowledgment Order
	13	07:34.34	r-dsch	PDU	Order Message	Connect Order
	14	07:34.70	f-dsch	PDU	Order Message	Base Station Acknowledgment Order

Messages that follow the ladder diagram

Pilot strength messages that have been added by 8960

Messages that are optional – not on ladder but included in 8960

Agilent Technologies

This is a view of a stored file from the Wireless Protocol Analyzer. It is the call scenario shown a few slides ago with the ladder diagram.

The editing I have done to generate this slide are limited to truncation of several columns on the right that identified the direction of the message, and adding the color codes. The time stamp information was formatted to show 2 decimal places, rather than the Microsoft default of one.

The messages in black match exactly those on the ladder diagram. Those in red have been added by the test set so that an updated message of the status of the phone's link is displayed. The messages in blue are optional in the system, our implementation turns them on.

The total time between the page message and the ringing of the phone (Alert with information message) is just under 1.7 seconds. At this point in the log, there is a 3 second delay, which corresponds to the system waiting for me to pick up the call.

The star in the upper left has been added for this presentation; that message was selected and displayed in detail, shown on the next two slides.

Details of the General Page Message (1)

6	00000000	00	MTAL Event Type=PDU
7	00000001	01	Channel Type=f-csch (F-PCH)
8	00010010	12	MSG_LENGTH=18(dec)
9	00010001	11	f-csch MSG_TYPE=General Page Message
10	000100--	10	CONFIG_MSG_SEQ=4
	------00		ACC_MSG_SEQ=2
11	0010----	2e	
	----1---		CLASS_0_DONE=1
	-----1--		CLASS_1_DONE=1
	------1-		TMSI_DONE=1
	-------0		ORDERED_TMSIS=0
12	1-------	80	BROADCAST_DONE=1
	-0000---		RESERVED=0
	-----000		ADD_LENGTH=0
13	0010----	25	PAGE_CLASS=Class 0, IMSI_S and MCC included
	----010-		MSG_SEQ=2
	-------1		MCC= 000

This slide has only been edited to choose font and size of text. It is rather small for a presentation, but the details of the contents are not really the point here.

On the right hand side is a listing of each field in the message using the exact name from the standard, and the value that has been sent in the message being decoded.

On the left are decimal, binary, and hex representation of the data. In the binary view, the packing of different fields are shown. Many of the fields are only one bit wide, typically an ON/OFF or Yes/No indication.

Details of the General Page Message (2)

14	11110011	f3	
15	1-------	fc	
	-1111100		IMSI_S= 0000009811
16	11111111	ff	
17	00111100	3c	
18	11010111	d7	
19	100-----	90	
	---1----		SDU_INCLUDED=1
	----0000		SERVICE_OPTION=3(dec)=Enhanced Variable Rate Voice Service (8 kbps)
20	00000000	00	
21	0011----	30	
	----0000		PADDING=0
22	00------	32	
	--110010		CRC=321ea914(hex)
23	00011110	1e	
24	10101001	a9	
25	00010100	14	

This is a continuation of the message started on the prior slide. The Cyclical Redundancy Check (CRC)is included. This is a layer 3 CRC, and is different from the layer 1 CRC used by the physical layer.

Layering Note: In the OSI model, the CRC is a layer 2 function. In cellular systems, this is typically pushed to layer 1 as it is implemented in hardware rather than software. In cdma2000 traffic channels, the layer 1 physical layer CRC is 12 bits long, while the CRC on messages is 16 bits long. On the control channels, there is only the layer 3 CRC, and it is 30 bits long.

Why is This Important?

- **Any wrong field or message causes a dropped call – with no error message**
- **Logging only at the MS will miss inconsistencies**
- **Ability to capture, evaluate, and document errors is important**
- **More engineering in implementation of protocols and data applications than in RF**

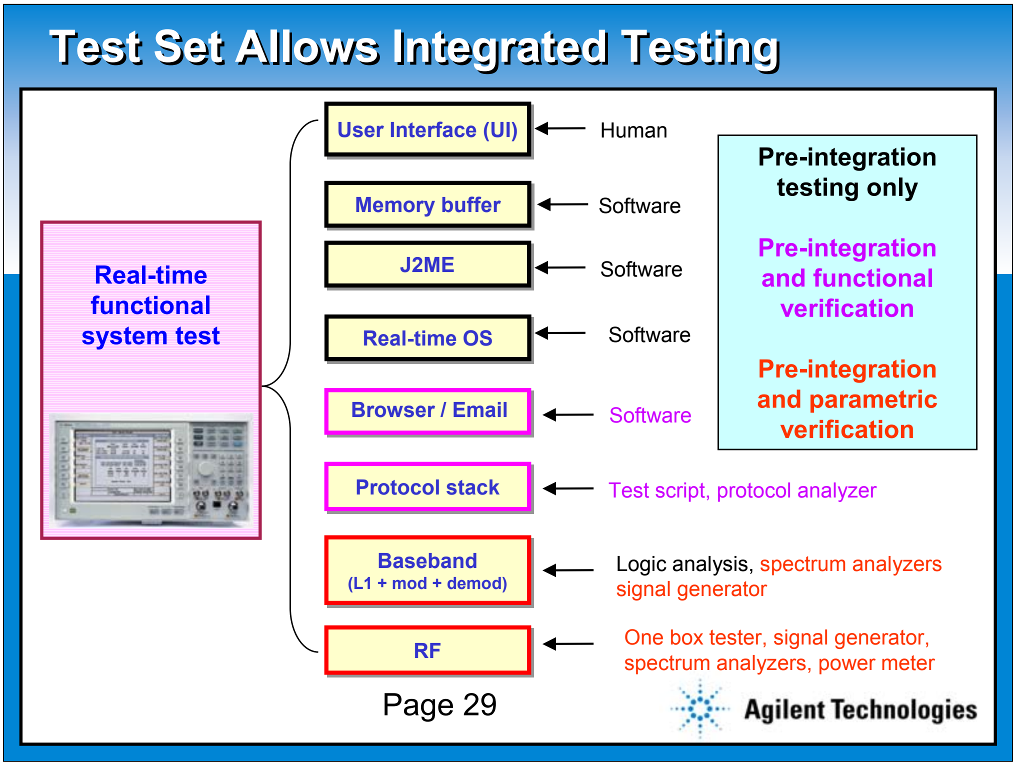
Agilent Technologies

One rule of wireless protocols is that a call must be dropped if anything improper happens. A dropped message is not considered improper. An improper message, or an inconsistent field content can cause this action. It is difficult to troubleshoot this type of problem, as the action of the phone is to suddenly send a disconnect message and leave the link. There are no error messages or trace as to why this happens.

Most phones have the ability to log the protocols as sent and received by the phone. This link is shared between the phone and the base station, so the logs should exactly match. The key word here is "should." It is very useful to see if the two ends have a mismatch, because that points to a problem.

The ability to capture complete call processing steps leading up to a bug is important in trying to re-create the action.

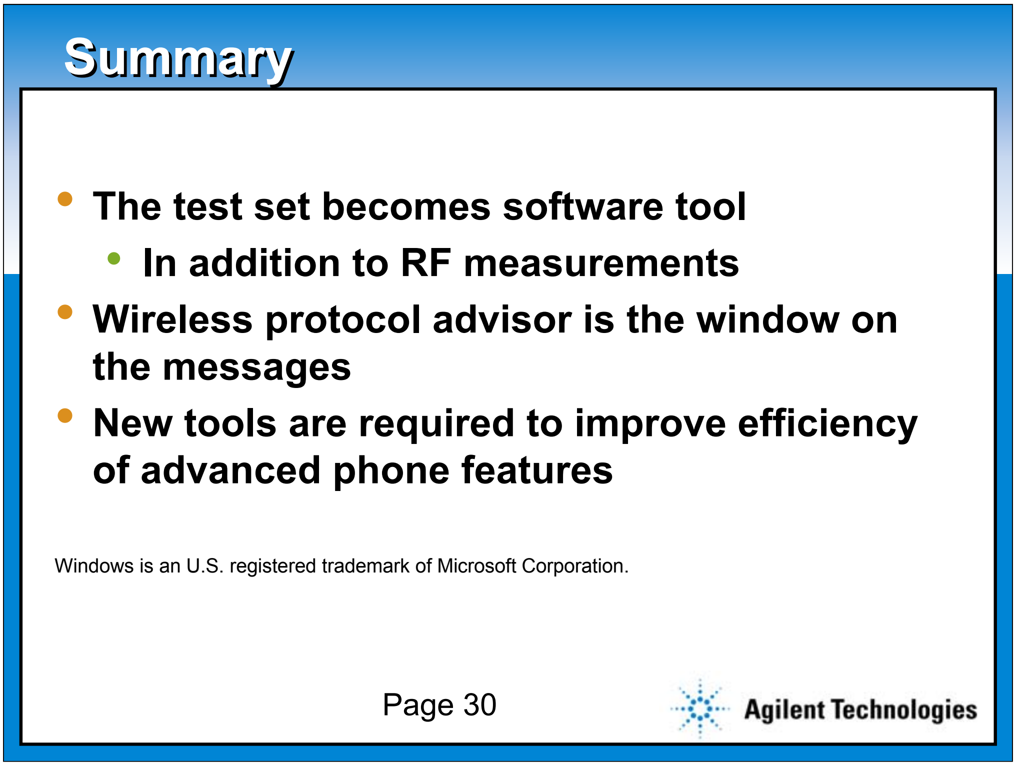
In modern phone R&D, there are many more engineers doing development work in the area of air link protocols and applications than in RF design and evaluation. The efficiency of this group of engineers is critical to meeting project schedules.



Many different elements of the phone design need testing and validation. Many of these are pure software implementations, and most of the testing can be done before integration. The proper action of these still need to be confirmed with an active RF link and real-world impairments.

RF testing is still needed, both to evaluate the RF circuitry and the baseband (layer 1) digital processing.

Having all this capability in one box is a plus. Setting up a link with a single button push allows the engineers to focus on design and validation job rather than spending time on the test environment.



While most people think of a test set as a radio frequency tester, the addition of protocol tools moves it into the software evaluation environment. Different version of the test set will either include or exclude the RF measurements. We call these Lab Applications or Protocol Applications.

The Wireless Protocol Advisor is valuable as a tool to monitor and analyze the messages.

New tools are needed to allow the engineering staff to be more productive and raise the probability of meeting the schedules.

Product Summary

System	Lab Application E5515C Mainframe	Protocol Application E6900A Mainframe
GSM/GPRS EGPRS	E6701C E6704A	E6910A (GPRS only)
W-CDMA	E6703A	E6912A
cdma2000	E6702A	E6911A

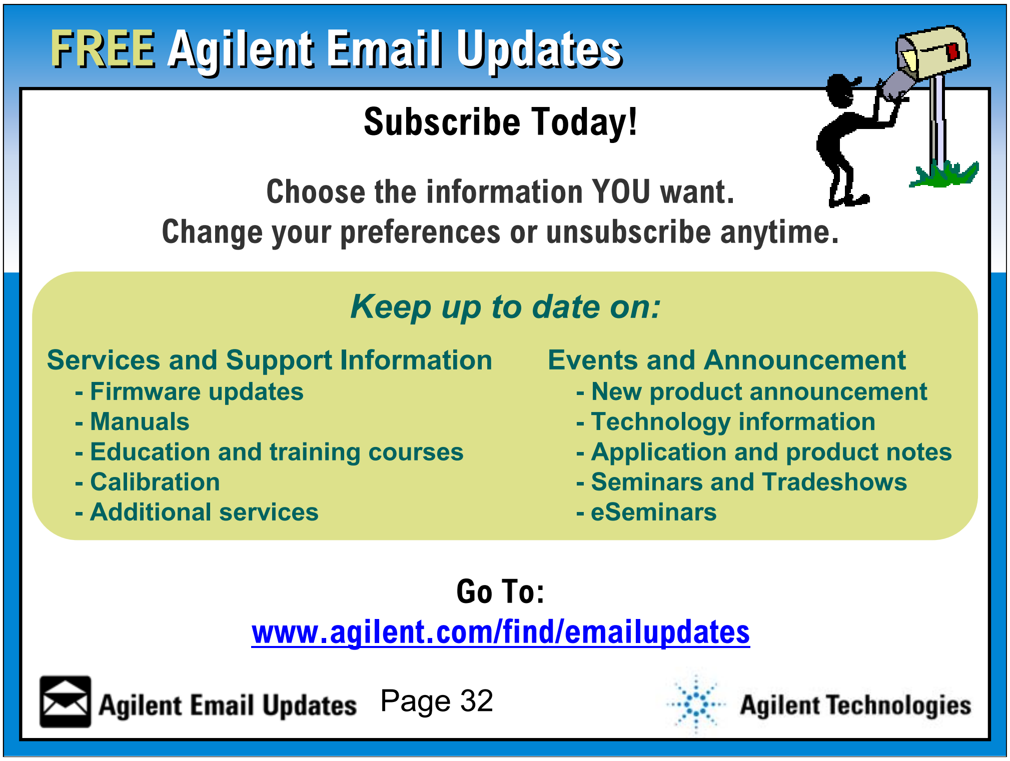
Lab Application: protocol logging *with* RF measurements

Protocol Application: protocol logging *without* RF measurements

Agilent Technologies

There are two mainframes from Agilent: The E5515C can be loaded with Lab Applications and have full RF test capabilities, as well. The E6900A does not have the RF test features, but instead is focused only on protocol test.

Either test set can support multiple radio formats, typically without hardware change. One option is needed to support the CDMA formats.



In a moment we will begin with the Q&A but 1st, for those of you who have enjoyed today's broadcast, Agilent Technologies is offering a new service that allows you to receive customized Email Updates. Each month you'll receive information on:

•Upcoming events such as eSeminars, seminars and tradeshows

•the latest technologies and testing methods

•new products and services

•tips for using your Agilent products

•updated support information (including drivers and patches) for your Agilent products

It's easy to subscribe and you can change your preferences or unsubscribe at anytime. Once you've completed the NetSeminar feedback form you will be directed to Agilent's resource page located on slide # XX, at that point simply click on the Agilent Email Updates link and you will be directed to the subscription site.

Now on to the feedback form then to Q&A……..