Agilent Technologies

Data Throughput Analysis on IS-2000 Wireless Networks

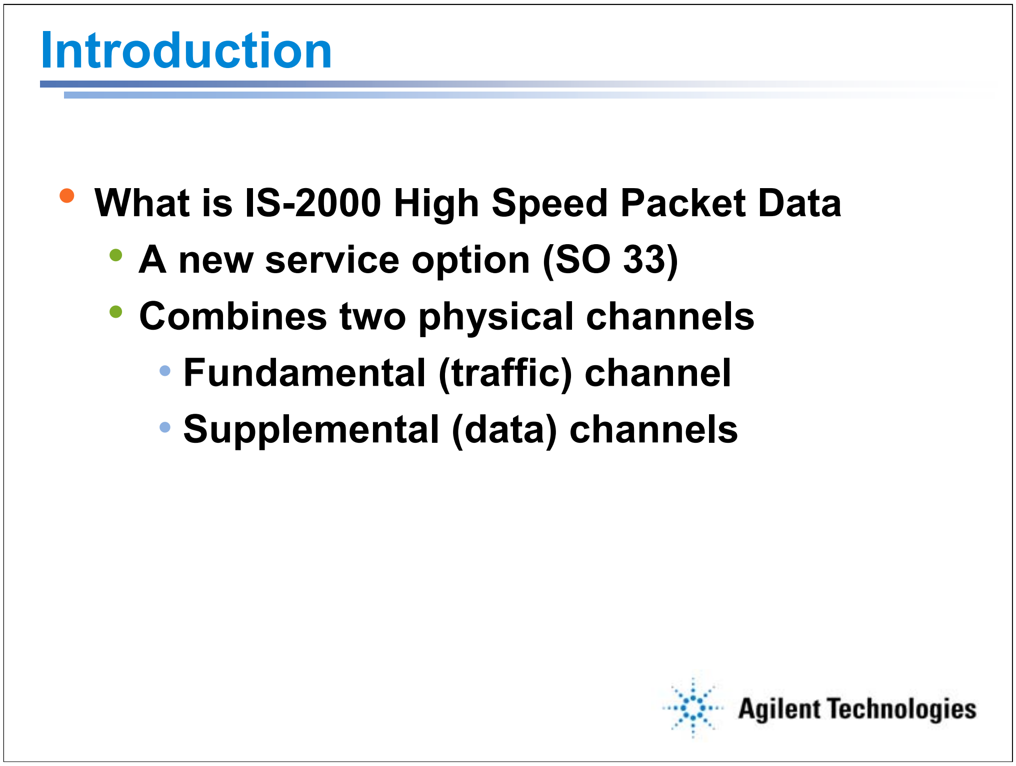
October 8th, 2003

presented by:

Paul Dohrman

Agenda

- Introduction
- What is packet switching?
- Network models
- Upper layer (end-to-end) protocols
- Lower layer protocols
- Analyzing data throughput



Introduction

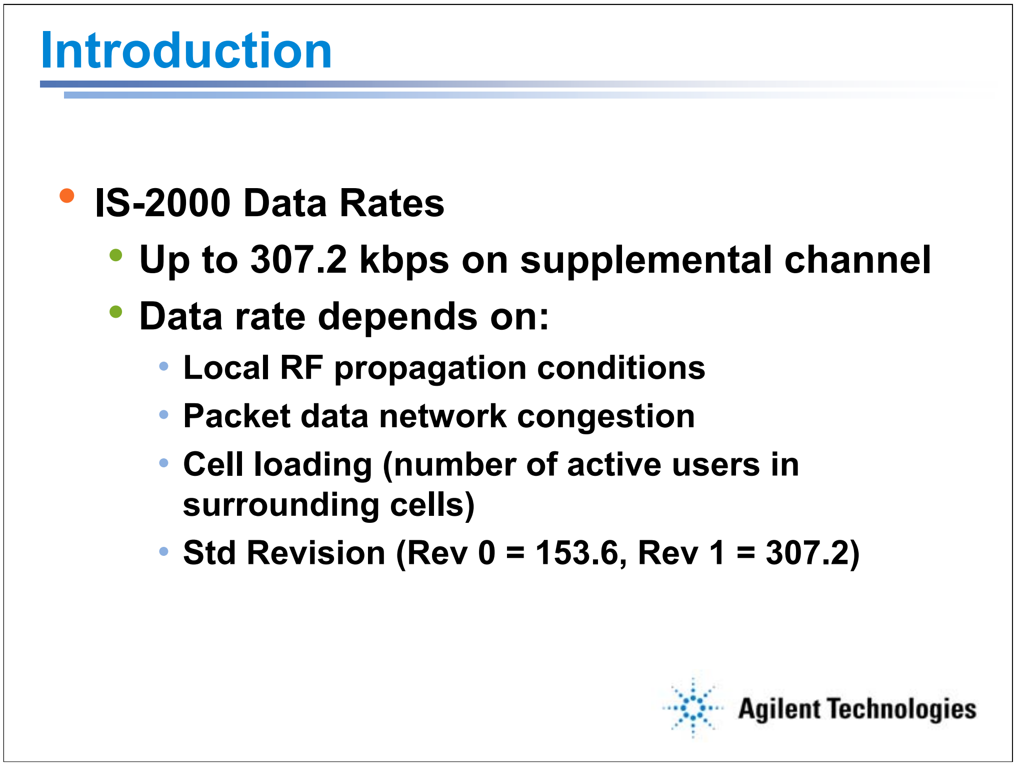
- What is IS-2000 High Speed Packet Data
    - A new service option (SO 33)
    - Combines two physical channels
        - Fundamental (traffic) channel
        - Supplemental (data) channels

Service options specify how traffic bits are processed by the wireless device and the base station. SO 33 configures the baseband processing software to handle high speed packet data.

SO 33 is available with radio configurations 3 and above. With SO 33, forward and reverse supplemental channels can be added to the fundamental (traffic) channel data rates to increase bandwidth.

The supplemental channels are requested by the mobile station when high speed operation is needed. The base station assigns the supplemental channel and controls the duration of time that the supplemental channel is granted.

The test set is limited to one supplemental channel.



Introduction

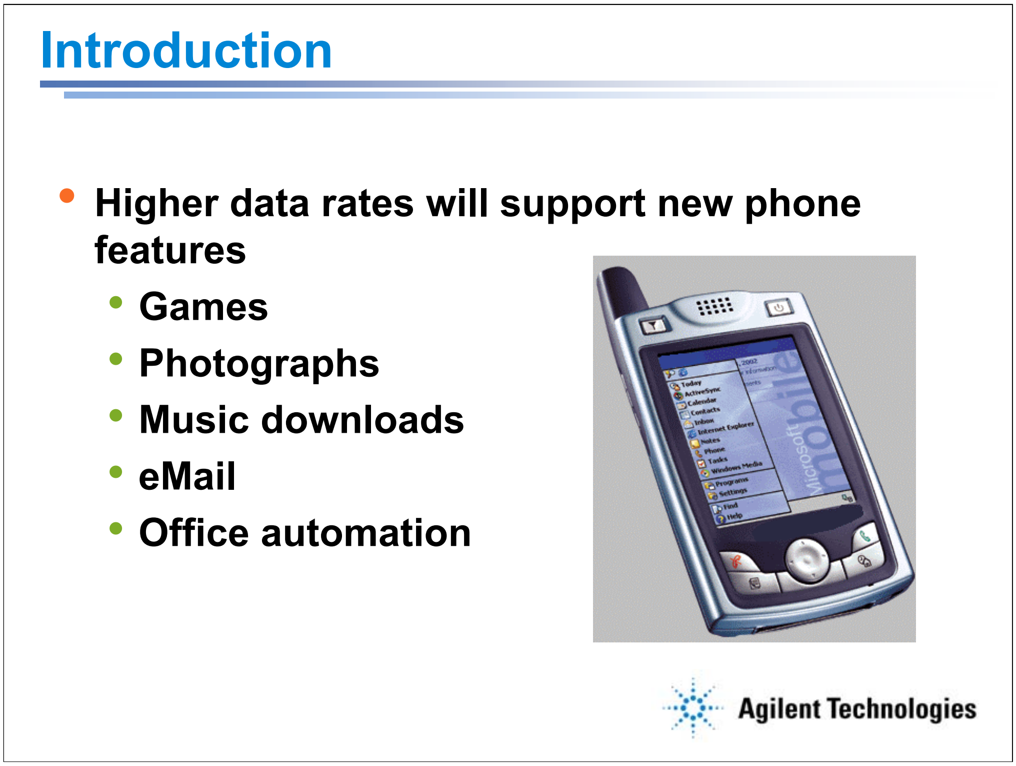
- IS-2000 Data Rates
  - Up to 307.2 kbps on supplemental channel
  - Data rate depends on:
    - Local RF propagation conditions
    - Packet data network congestion
    - Cell loading (number of active users in surrounding cells)
    - Std Revision (Rev 0 = 153.6, Rev 1 = 307.2)

Agilent Technologies

As higher data rates are granted, less Walsh code space is available for other traffic causing cell loading and reducing network capacity.

RF propagation conditions can disrupt the flow of data traffic by reducing the signal to noise (Eb/Nt) to a level that makes it impossible to decode data.

Network congestion can also reduce data flow, causing data to be transmitted multiple times before the receiving end acknowledges it.



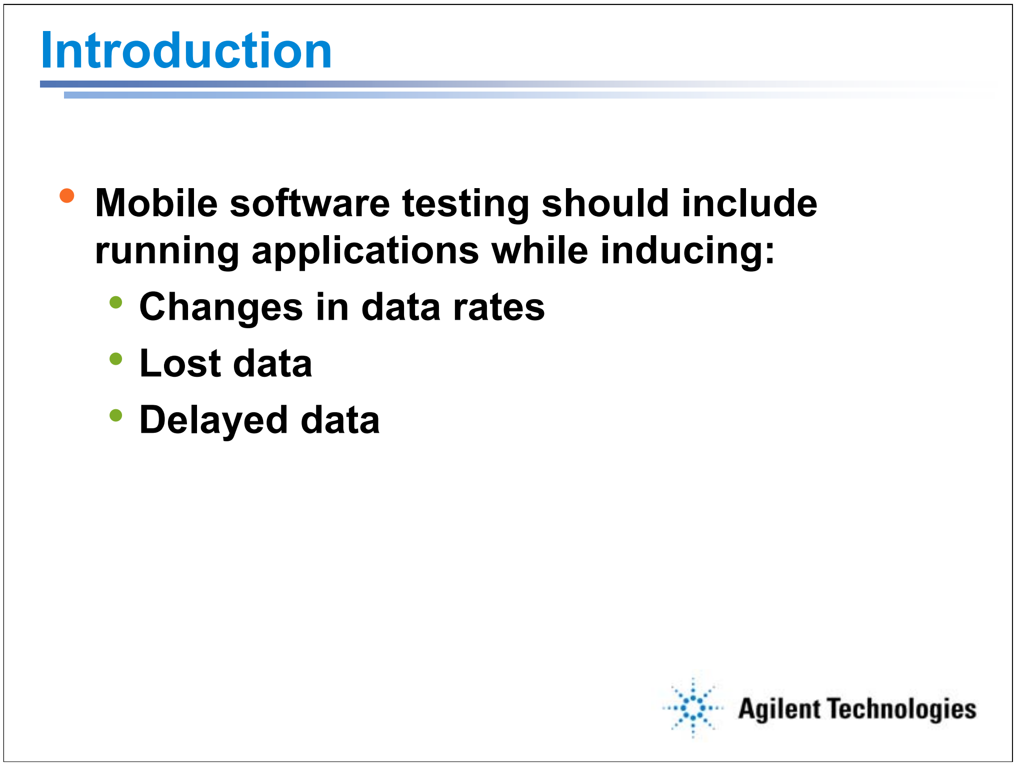
Introduction

- Higher data rates will support new phone features
  - Games
  - Photographs
  - Music downloads
  - eMail
  - Office automation

Agilent Technologies

Interactive and multimedia applications are appearing more often on wireless devices as data rates go up.

Java (J2ME) and Brew are a couple of popular programming languages approved by cell phone manufacturers. Wireless Application Protocol (WAP) provides standard specifications for displaying graphics on a small screen.



Introduction

- Mobile software testing should include running applications while inducing:
  - Changes in data rates
  - Lost data
  - Delayed data

Agilent Technologies

Software is often written by small companies with inadequate equipment to test the effects of variations in RF propagation conditions. In some cases, qualification labs are available to test software prior to releasing it to service providers for integration.

Effects of data rate variations include unacceptably long file downloads, graphics images that take too long to display, and streaming video images freezing.

Delayed data causes the mobile station to buffer data while waiting for the late packets to arrive.

Delayed data (due to retransmissions) can cause the mobile station's application to perform at a level that is unacceptable to the end user.

Introduction

Two powerful data diagnostic tools are available from Agilent:

1. E5515C c2k Lab Application

- **IP router (data channel)**
- **RLP data counters**
- **RF noise/level control**
- **Data rate control**

Agilent Technologies

The C2K Lab Application is the "network on a bench". It is useful when the performance of application software needs to be tested in a controlled environment.

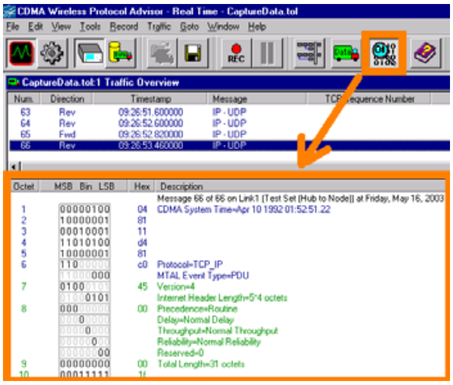
IP data can be routed through an Ethernet port to/from a wireless device through the RF port. Data transfer is monitored by RLP (Radio Link Protocol) counters, and the data rate can be changed while on a call.

RF power can be adjusted to simulate poor channel conditions and an AWGN (Additive White Gaussian Noise) noise source can be added to the signal to simulate signal interference.

Introduction

Two powerful diagnostic tools are available from Agilent Technologies:

2. WPA (Wireless Protocol Advisor)


CDMA Wireless Protocol Advisor - Real Time - CaptureData.tol
File Edit View Tools Record Traffic Goto Window Help
REC
CaptureData.tol:1 Traffic Overview

Num.	Direction	Timestamp	Message	TCP Sequence Number
63	Rev	09:26:51.600000	IP - UDP	
64	Rev	09:26:52.600000	IP - UDP	
65	Fwd	09:26:52.820000	IP - UDP	
66	Rev	09:26:53.460000	IP - UDP	

Octet	MSB Bin LSB	Hex	Description
			Message 66 of 66 on Link1 [Test Set [Hub to Node]] at Friday, May 16, 2003
1	00000100	04	CDMA System Time=Apr 10 1992 01:52:51.22
2	10000001	81	
3	00010001	11	
4	11010100	d4	
5	10000001	81	
6	11000000	c0	Protocol=TCP_IP
	11000000		MTAL Event Type=PDU
7	01000101	45	Version=4
	01000101		Internet Header Length=5*4 octets
8	00000000	00	Precedence=Routine
	00000000		Delay=Normal Delay
	00000000		Throughput=Normal Throughput
	00000000		Reliability=Normal Reliability
	00000000		Reserved=0
9	00000000	00	Total Length=31 octets
10	00011111	1f	

- **Message Logging**
- **Decode View**
- **Filters, triggers**
- **Post capture analysis**

Agilent Technologies

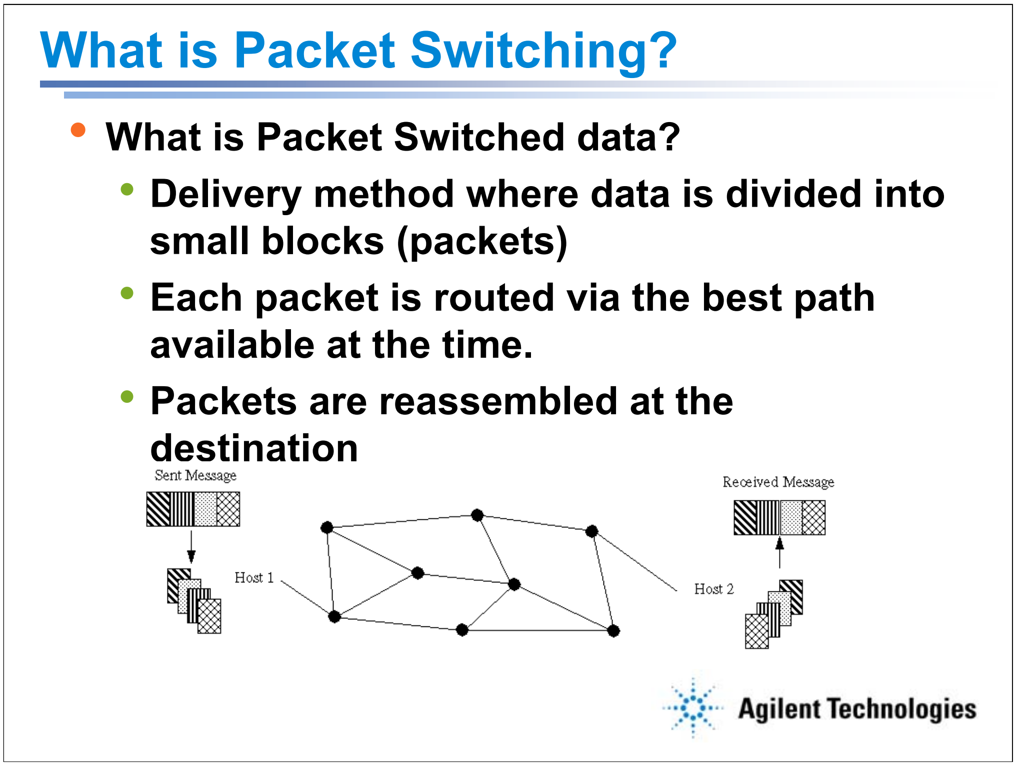
The WPA can monitor messages at various tap points in the protocol stacks. Unwanted messages can be filtered out and triggers can limit logging to time periods beginning just prior to or at a particular protocol event.

Data can be "unpacked" by opening the Decode View. Every byte is listed and labeled.

Agenda

- Introduction
- What is packet switching?
- Network models
- Upper layer (end-to-end) protocols
- Lower layer protocols
- Analyzing data throughput

Agilent Technologies



What is Packet Switching?

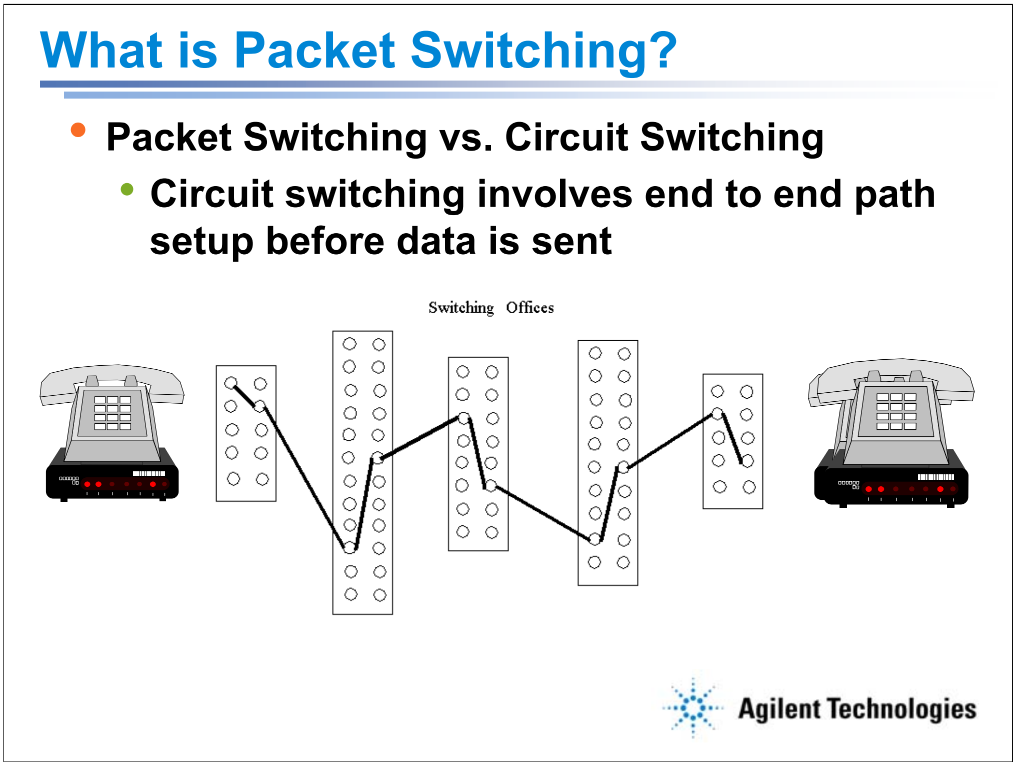
- What is Packet Switched data?
  - Delivery method where data is divided into small blocks (packets)
  - Each packet is routed via the best path available at the time.
  - Packets are reassembled at the destination

Agilent Technologies

A quick overview of packet switched data will be helpful in understanding how lost/delayed packets affect throughput.

Packet data usually refers to the network layer peer to peer exchange of packets of data. Packet size is limited (typically not much larger than 1 kB) and each packet is sent with enough control information for the network to route each packet individually to the receiver on the other end.

Protocols are designed to receive packets in a different order than they were sent and to re-assemble them in the correct order.



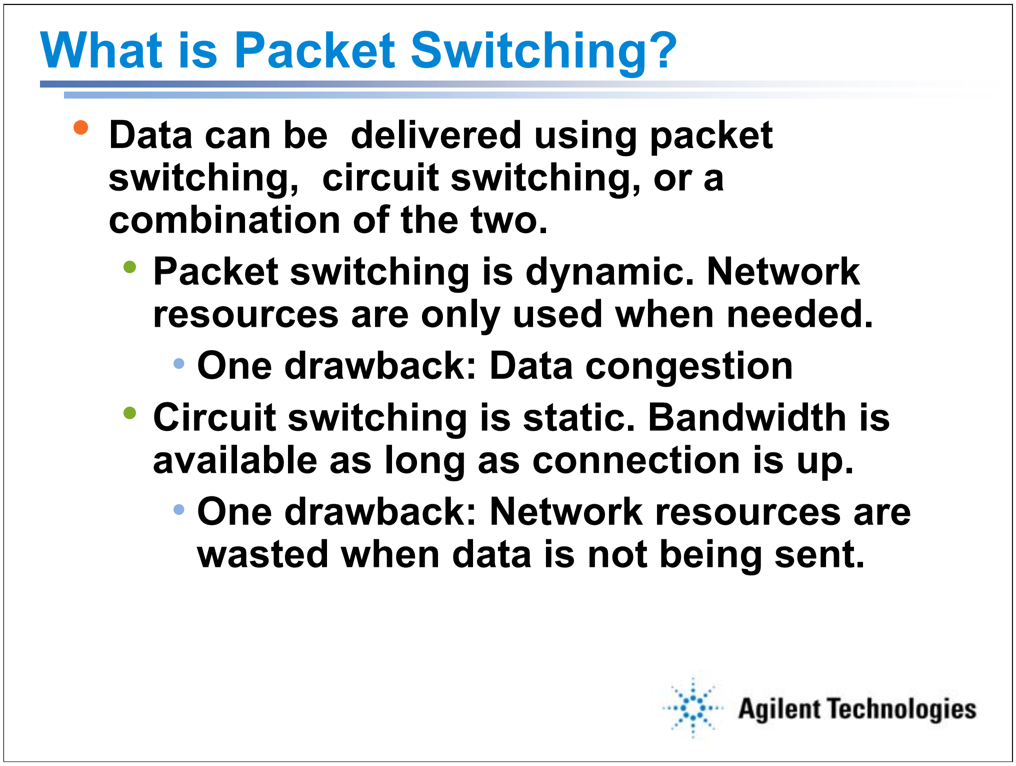
What is Packet Switching?

- Packet Switching vs. Circuit Switching
  - Circuit switching involves end to end path setup before data is sent

Circuit switching takes time to set up, sometimes on the order of 10 seconds.

ISDN is a good example of circuit switching, although ISDN data can be routed to packet switched connections.

Once a call is made voice and data can be transmitted on the same circuit. The medium over which the data flows is conceptually referred to as a "digital bit pipe"



What is Packet Switching?

- Data can be delivered using packet switching, circuit switching, or a combination of the two.
  - Packet switching is dynamic. Network resources are only used when needed.
    - One drawback: Data congestion
  - Circuit switching is static. Bandwidth is available as long as connection is up.
    - One drawback: Network resources are wasted when data is not being sent.

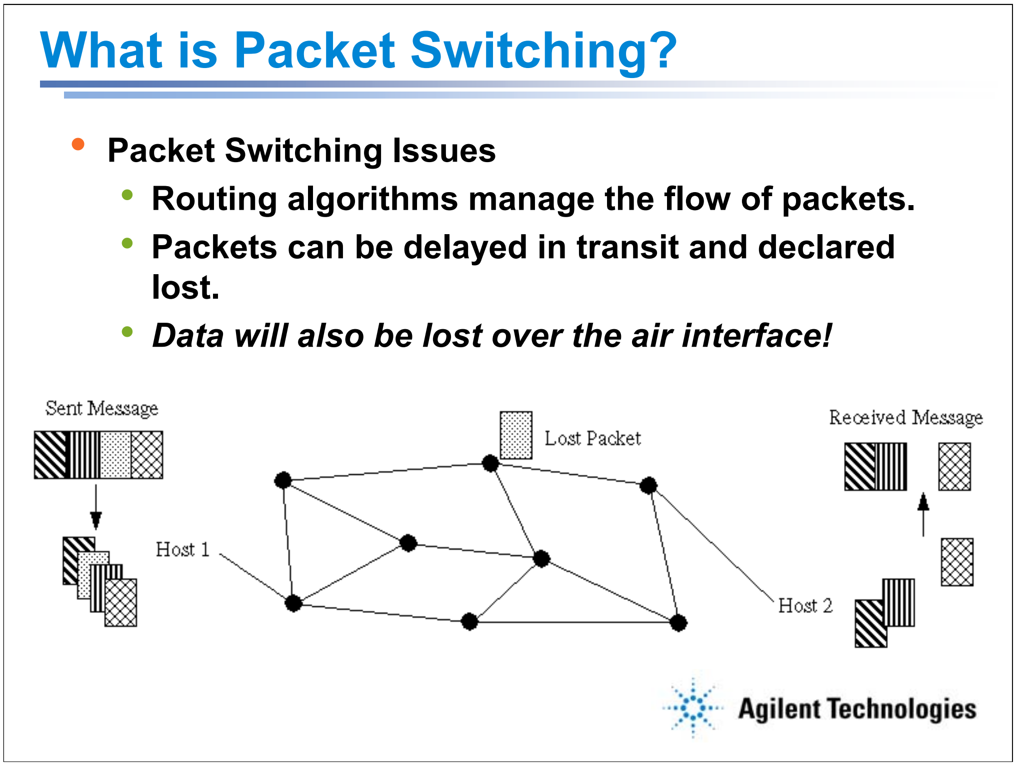
Agilent Technologies

For bursts of data, packet switching makes more efficient use of network bandwidth than the alternative, circuit switching.

Circuit switching requires a constant connection (data path) which takes time to set up and wastes bandwidth during quiet periods. Once it is established, however, there is no problem with congestion or data getting out of sequence.

If data is being sent by a mobile station over the wireless medium, a dedicated physical connection is established, but it is usually relaying packet data bound for the packet internet.

The wireless medium is an inherently unreliable path and data loss is likely to occur.



What is Packet Switching?

- Packet Switching Issues
  - Routing algorithms manage the flow of packets.
  - Packets can be delayed in transit and declared lost.
  - *Data will also be lost over the air interface!*

Complex routing algorithms are used to make decisions about the best path to send packets on. If the algorithms work, packet data travels on the most efficient, least congested route. If not, data is slowed dramatically. This can occur when too many packets are routed to one particular node, causing network congestion. Packets can be delayed so long that they are declared lost.

In a wireless application, data loss is mostly due to RF propagation conditions. Network problems such as congestion only add to the problem of data delivery.

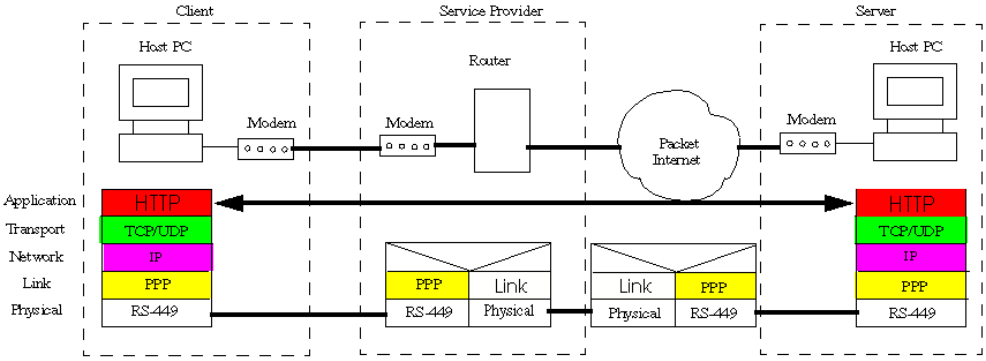
Agenda

- Introduction
- What is packet switching?
- **Network models**
- Upper layer (end-to-end) protocols
- Lower layer protocols
- Analyzing data throughput

Agilent Technologies

Network Model

- **Wireline network - dial up modem access**



Agilent Technologies

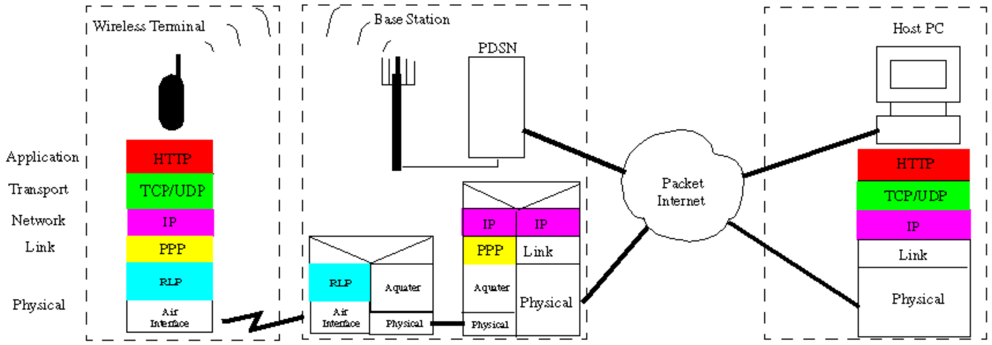
This graphic illustrates an “end to end” packet data communication network.

At one end is a typical PC (not on a LAN) accessing the Internet via a dial up modem connection to a local ISP (Internet Service Provider). All data transfer is over “copper” (no wireless links).

The color coded blocks highlight the protocol layers with peer to peer communication that is particularly relevant to each network entity.

Network Model

- **Wireless network - mobile access**

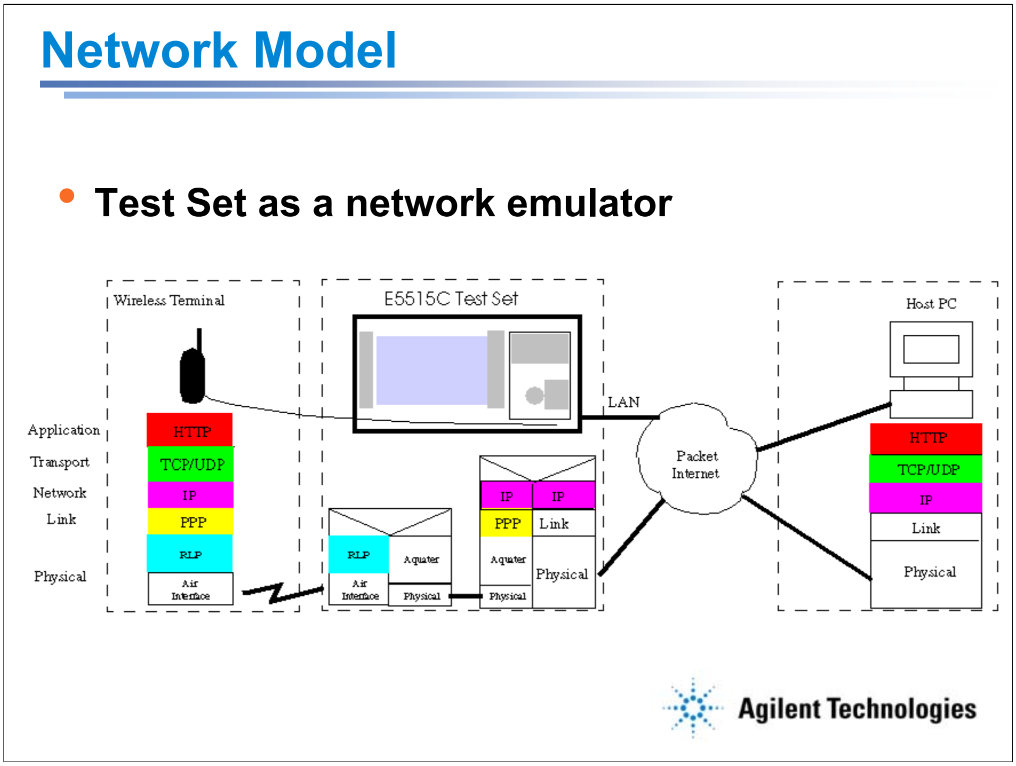


Agilent Technologies

In contrast with the previous slide, this model introduces the air interface, in place of the modem-modem link in the wireline version.

The physical layer in this network model is referred to as the relay layer to the PDSN. Central to the relay layer is the RLP (Radio Link Protocol), the protocol that is used to frame the data for streaming onto the CDMA physical channels. The combination of RLP and the air interface can be thought of as analogous to the modems in the prior slide.

The air interface represents the weak link in the chain of interconnections necessary to transport data from sender to receiver. This is where the test set can simulate real world network problems in a bench top environment.



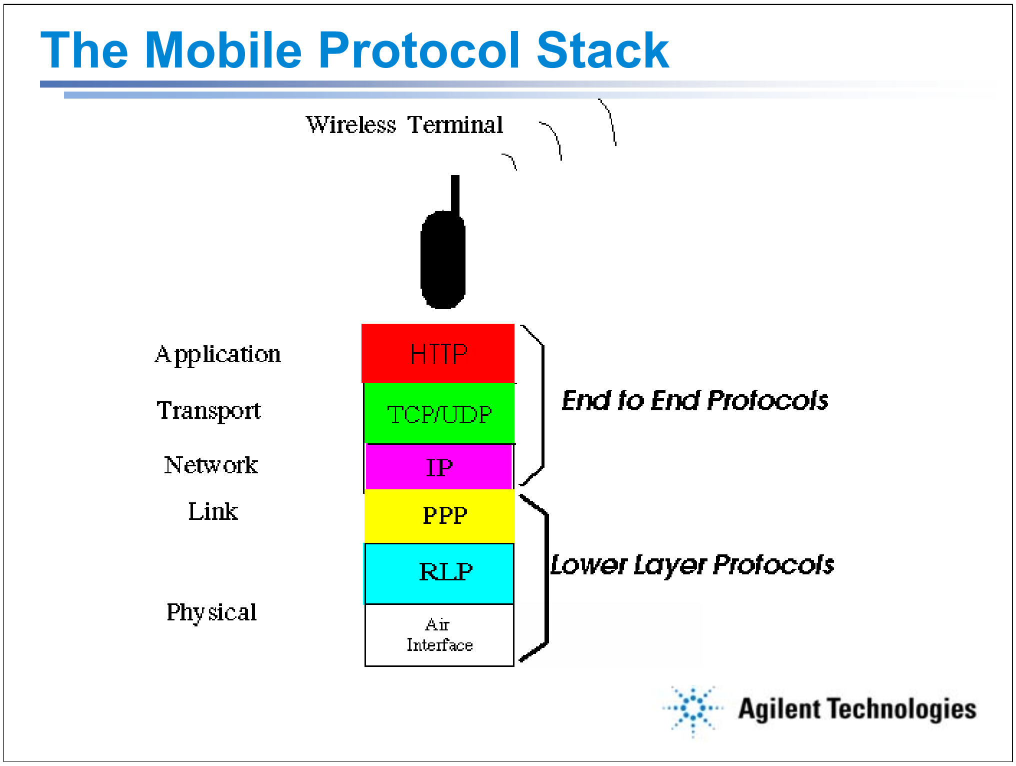
Network Model

- **Test Set as a network emulator**

Agilent Technologies

The test set performs the relevant functions of the PDSN, base station, mobile station controller, and PCF (Packet Control Function). IP datagrams are routed through the ethernet connection and through the RF interface to the mobile station.

The test set also has an internal http server. There is a home page and the capability to serve screen images.



The Mobile Protocol Stack

Wireless Terminal

Application — HTTP

Transport — TCP/UDP

Network — IP

Link — PPP

RLP

Physical — Air Interface

End to End Protocols

Lower Layer Protocols

Agilent Technologies

The network model for the SO33 protocol stack in the mobile station can be viewed in two groups.

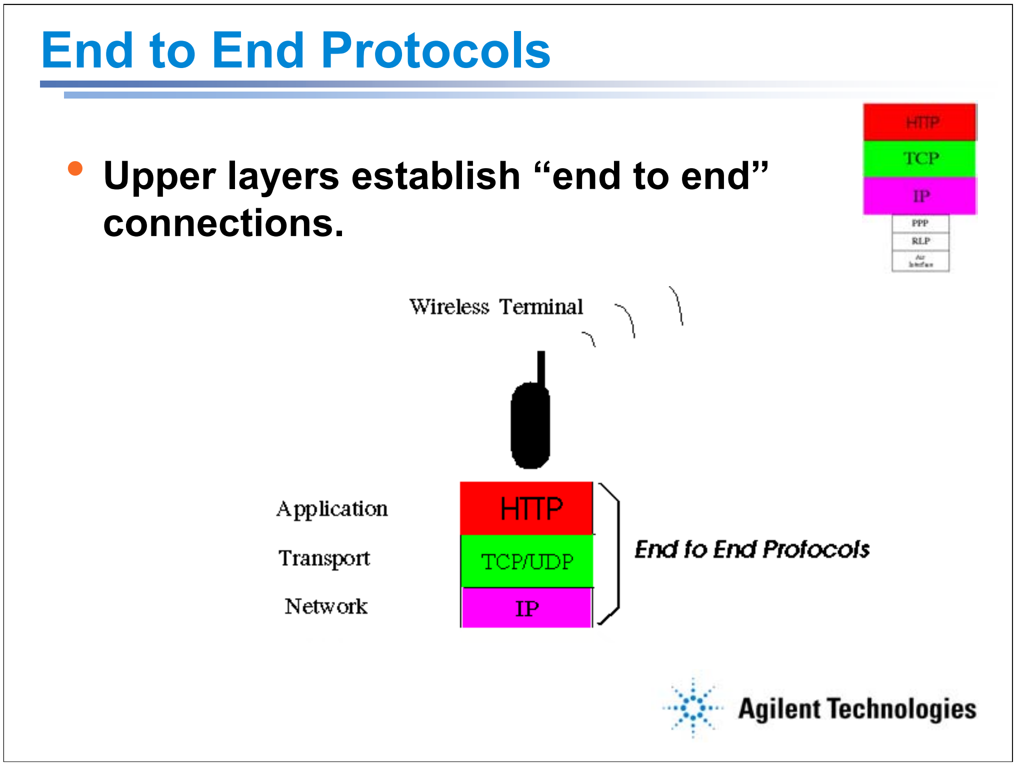
The upper layers must include control information in messages that support the routing of data to and from its final destination.

The lower layers are only concerned with establishing a “single hop” communication channel.

Agenda

- Introduction
- What is packet switching?
- Network models
- **Upper layer (end-to-end) protocols**
- Lower layer protocols
- Analyzing data throughput

Agilent Technologies



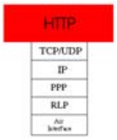
End to End Protocols

- Upper layers establish “end to end” connections.

For one application to communicate with another, the services of all layers below it are required.

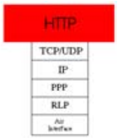
The application layer interfaces directly with TCP/UDP through protocol ports. TCP/UDP passes data to the IP network layer for packetization and routing to its destination.

End to End Protocols



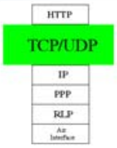
- Application Layer
  - Example application layer protocols
    - HTTP
    - WAP
    - SMTP
    - TELNET
    - FTP

End to End Protocols



- Application layer
  - End results of data disruptions are observed here
    - Excessive file download times
    - Image freezing during streaming video

End to End Protocols

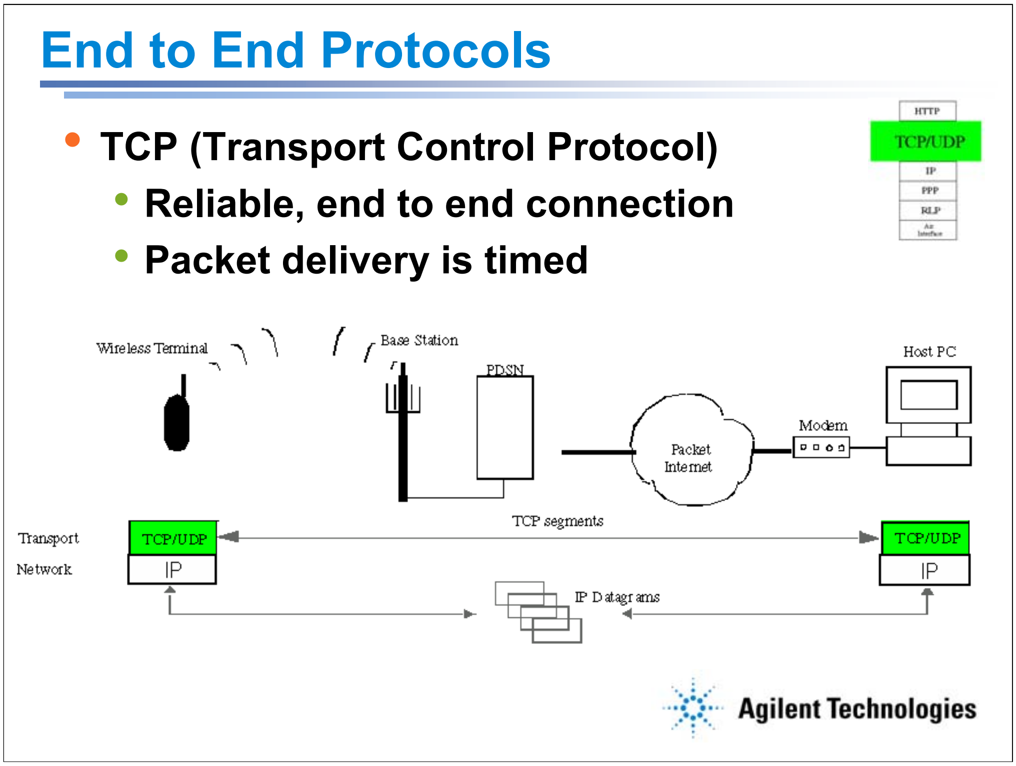


- TCP (Transport Control Protocol) layer
  - TCP reads data from the application layer and divides it into segments.
  - TCP relies on the services of the IP layer below it. IP encapsulates TCP segments within packets.
  - TCP is “connection oriented”

Agilent Technologies

TCP is a connection oriented protocol. By connection oriented, it means that data that is declared lost gets retransmitted. There is data acknowledgement and flow control. This attribute relieves the upper (application) layer of the complexities associated with fixing problems that come up as a result of unreliable channel characteristics.

In the TCP layer, each segment is sent with header information. In the header is a hexadecimal number that identifies the first byte of information. In the next segment, this number is incremented by the number of bytes sent in the last segment so that every byte is essentially numbered. Also sent in each segment is a “piggybacked” acknowledge number.The acknowledge number lets the other end know the sequence number of the next byte it is expecting.



End to End Protocols

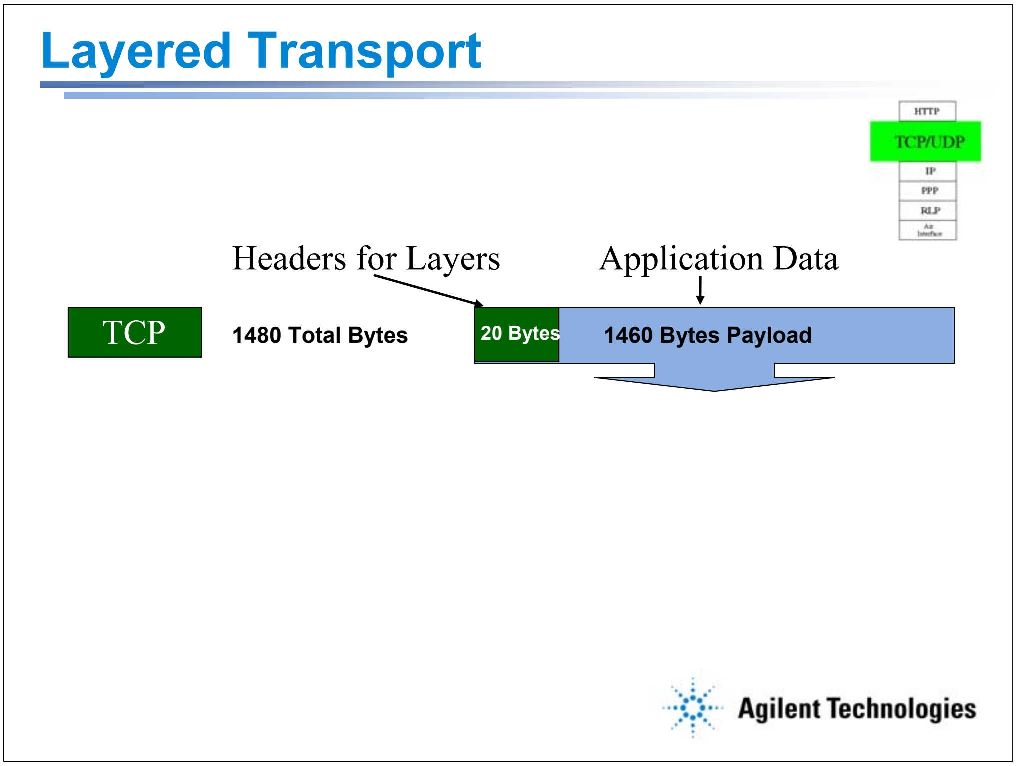
- TCP (Transport Control Protocol)
  - Reliable, end to end connection
  - Packet delivery is timed

TCP is a full-duplex, connection oriented protocol.

Data from an application is divided into segments, assigned a sequence number, and sent to a receiver host, encapsulated in IP datagrams.

If a segment is not acknowledged from the receiver by a predetermined length of time a timeout occurs. The TCP sender assumes there is congestion and waits a required amount of time (determined by a congestion window) before attempting to send the next segment.

With each segment sent, the TCP sender indicates how much data it can currently accept (flow control) when it receives its next segment. If this receive window goes to 0, data transfer is suspended until the TCP sender determines the receiver once again is ready to receive.

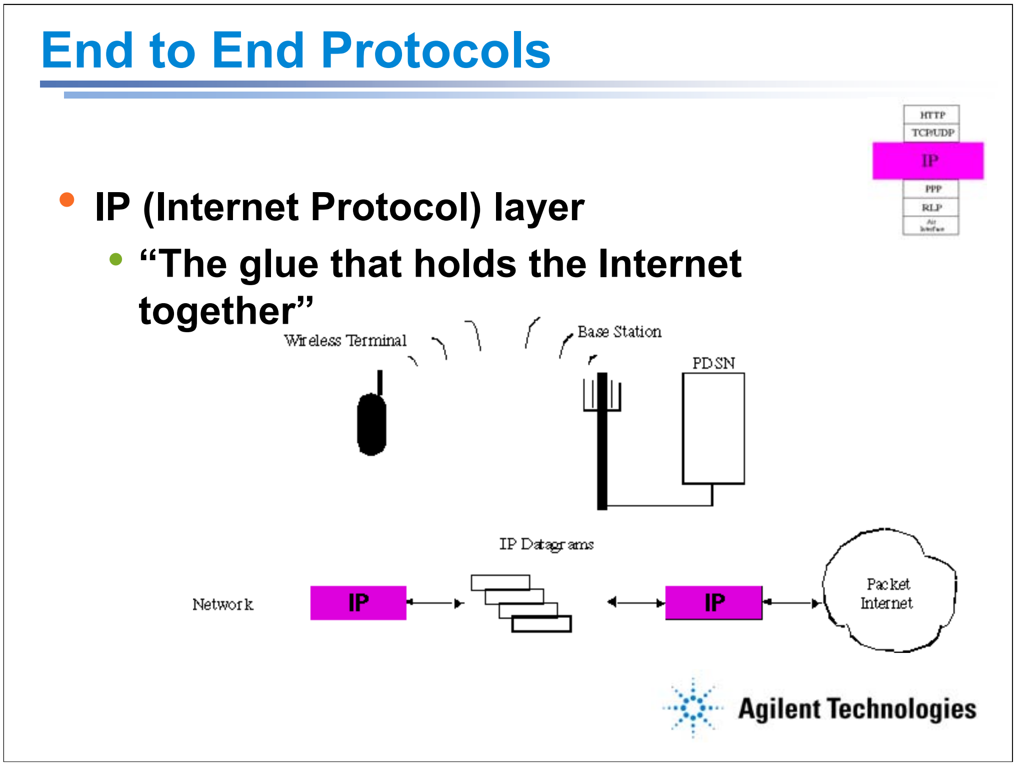


Layered Transport

Agilent Technologies

The TCP segment consists of a 20 byte header and 1460 bytes of application layer “payload”.

TCP does not care about frame boundaries established by the layer above. It simply divides the application layer data up into the size of blocks that are most efficient for transport and provides reliable, connection oriented service.



End to End Protocols

- IP (Internet Protocol) layer
  - "The glue that holds the Internet together"

Agilent Technologies

The IP layer packetizes datagrams sent from the upper layers.

It provides a "best effort" way to transport datagrams from the TCP/UDP layer across networks. Part of this task is figuring out the path with least congestion.

Packet ordering and flow control are not performed by IP. It is connectionless.

The headers added by IP provide instructions about how to handle the packets:

*What is its source address

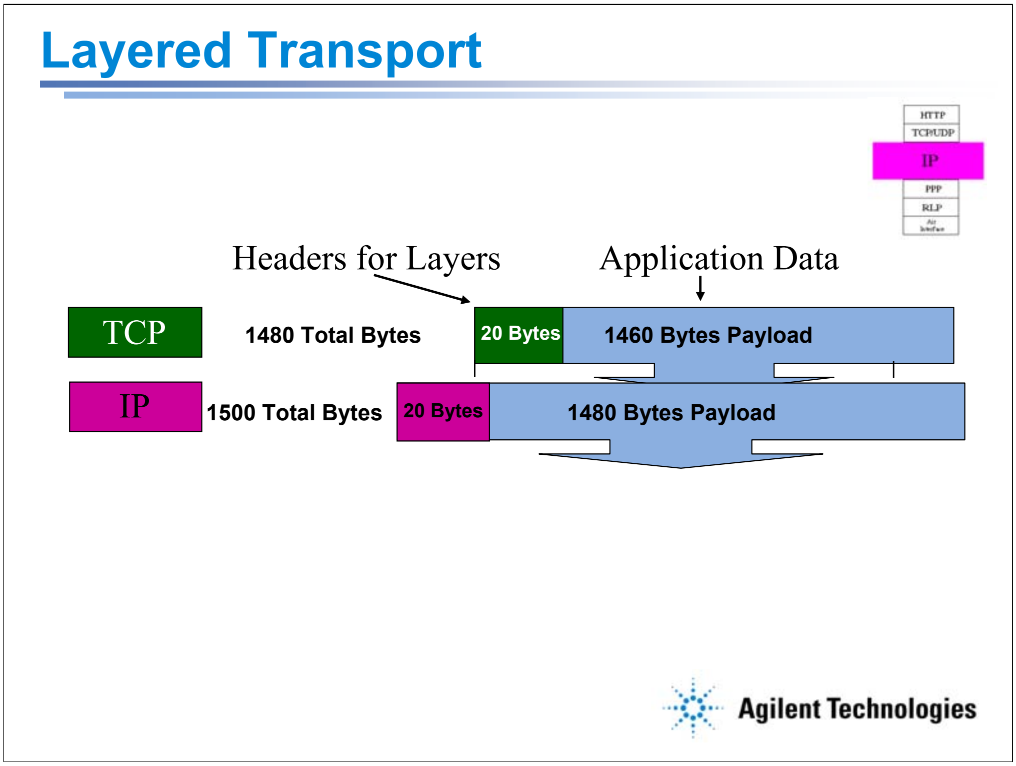
*What is its destination address

*Which piece of a datagram is it?

*Is speed more important than reliablility?

*Is it TCP or UDP?

Mobile IP adds the ability to manage hosts that move from one location to another. Home agents keep track of hosts whose home is in their area, but who are currently visiting another area. Foreign agents keep track of hosts who are from another area. When a message arrives for the travelling host, the home agent forwards it to the foreign agent and the foreign agent delivers it to the host.



Layered Transport

HTTP

TCP/UDP

IP

PPP

RLP

Air Interface

Headers for Layers

Application Data

TCP

1480 Total Bytes

20 Bytes

1460 Bytes Payload

IP

1500 Total Bytes

20 Bytes

1480 Bytes Payload

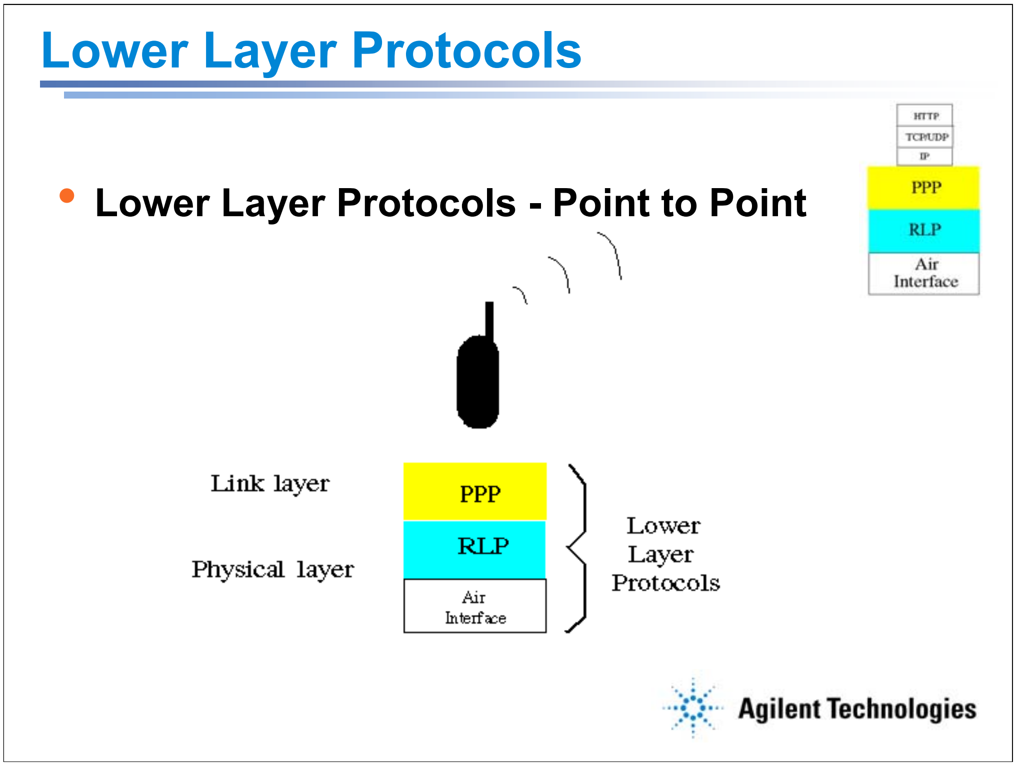
Agilent Technologies

IP adds 20 bytes of header information to form an IP datagram.

Agenda

- Introduction
- What is packet switching?
- Network models
- Upper layer (end-to-end) protocols
- Lower layer protocols
- Analyzing data throughput

Agilent Technologies



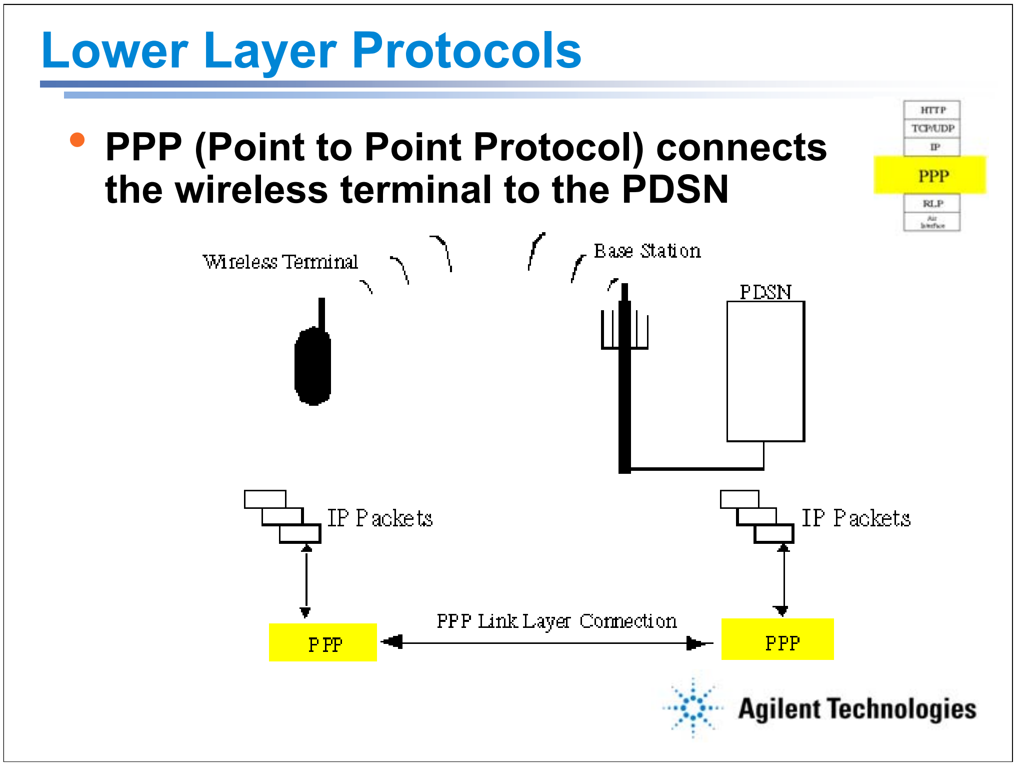
Lower Layer Protocols

- **Lower Layer Protocols - Point to Point**

The lower layer protocols support the exchange of data over a single hop. In the case of the wireless terminal the single hop is to/from the PDSN.

The RLP layer is similar to TCP in many ways. It divides PPP frames into smaller RLP frames and streams the data bytes from sender to receiver while providing error control within the limits of its ability to buffer data.

The air interface (IS-2000) is the lowest level protocol and specifies the method that binary data gets from one radio to another.



Lower Layer Protocols

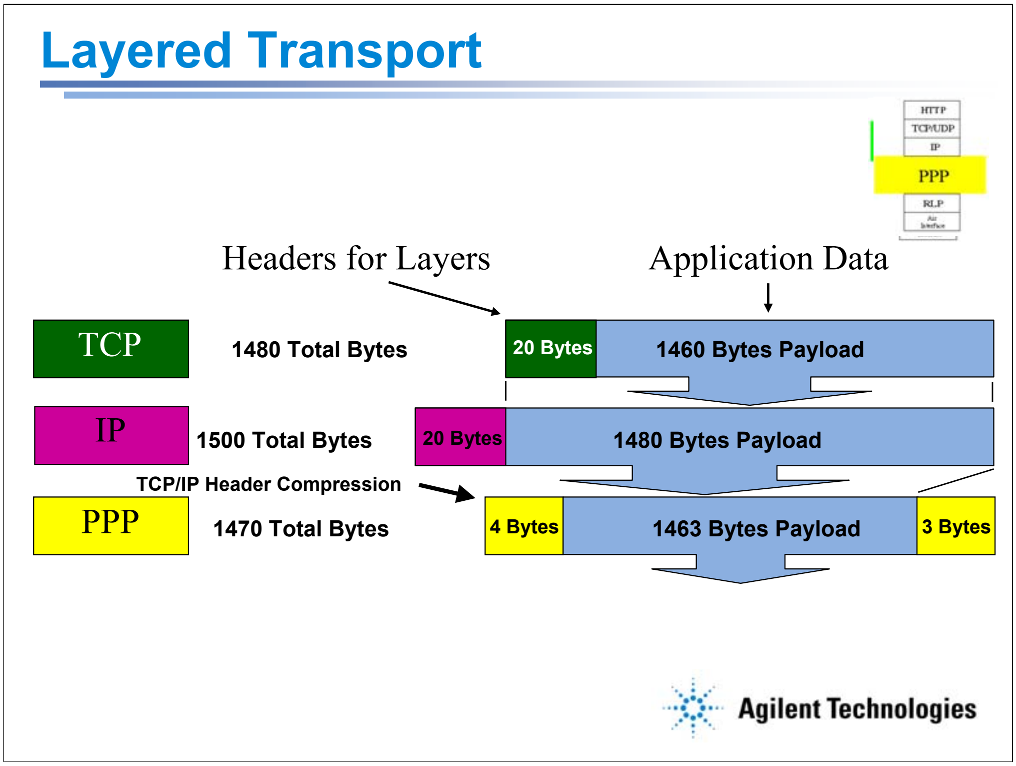
- PPP (Point to Point Protocol) connects the wireless terminal to the PDSN

Agilent Technologies

PPP establishes a connection between the wireless device and the PDSN and sends IP packets over the link layer connection. PPP is the same protocol that dial-up modems use to connect to the Internet service provider's router, and it is PPP that handles IP address negotiation for Internet service providers.

Point to point means that link layer peers communicate over a channel that directly connects the sender and receiver. There is no endpoint addressing or routing as with the IP network layer.

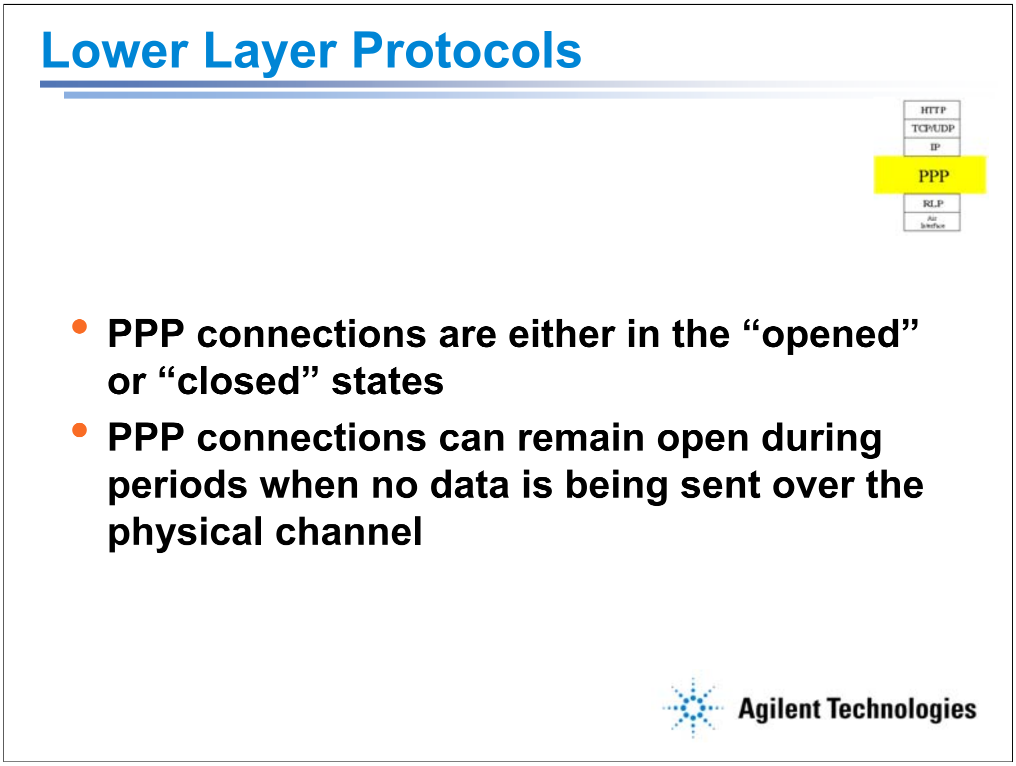
Also, the data link assumes that data is delivered in the same order it is sent unlike end-to-end packet data protocol layers like TCP, which expects segments to get out of order in transit.



Layered Transport

PPP accepts IP packets (IP datagrams are encapsulated within the packets), and maps them to PPP frames.

PPP can apply header compression. In this example, Van Jacobsen compression reduced 40 Bytes of TCP/IP header into 4 Bytes.



Lower Layer Protocols

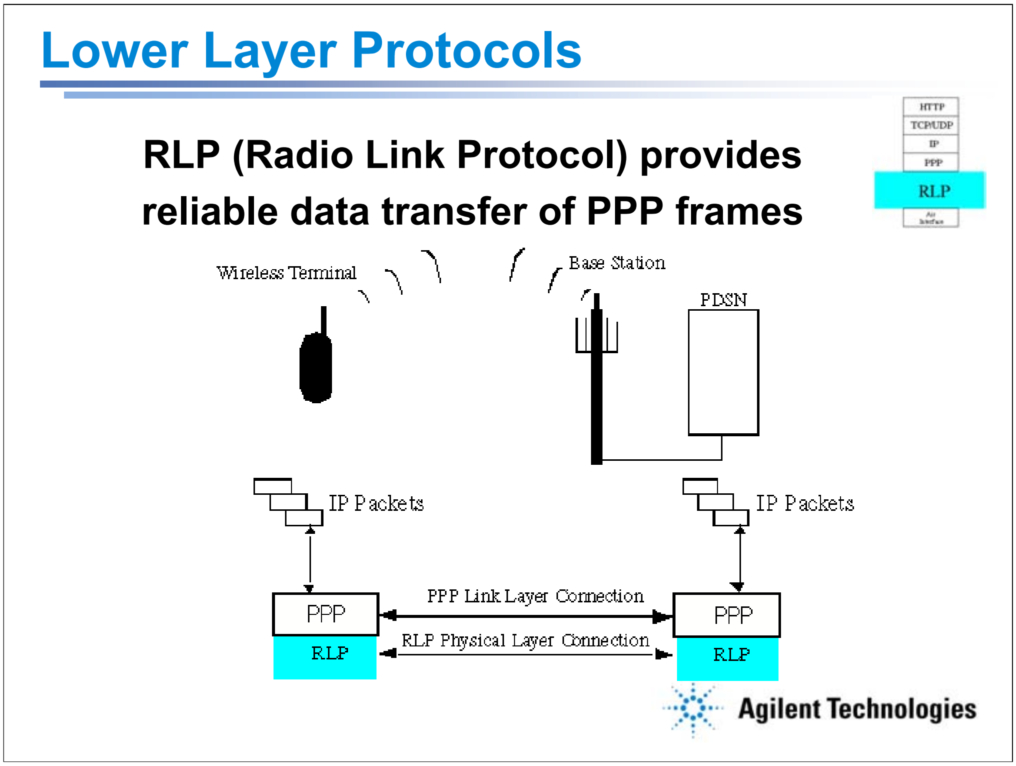
HTTP
TCP/UDP
IP
PPP
RLP
Air Interface

- PPP connections are either in the “opened” or “closed” states
- PPP connections can remain open during periods when no data is being sent over the physical channel

Agilent Technologies

When you are using a phone as a modem, the phone display may show “PPP” after the PC has requested a network connection.

Timers may (optionally) determine when data transfer has stopped and put the connection into a dormant state. The PPP connection remains opened during this time but the physical channel resources are released to handle other forms of traffic.



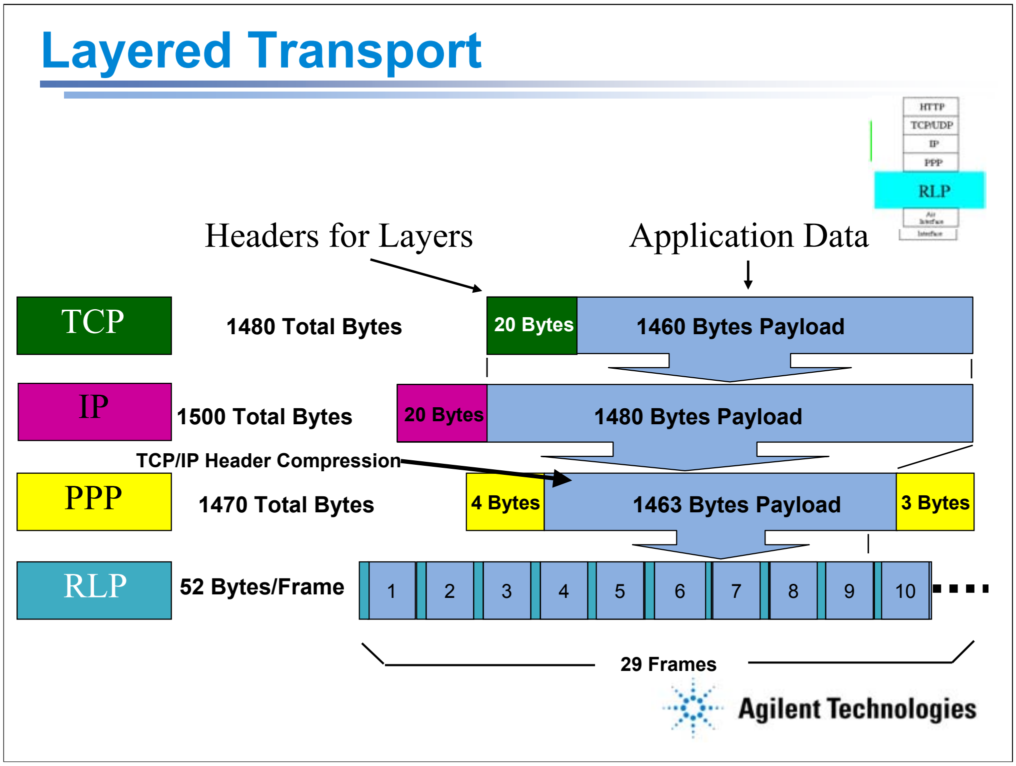
Lower Layer Protocols

RLP (Radio Link Protocol) provides reliable data transfer of PPP frames

Agilent Technologies

RLP divides PPP frames into RLP frames.

RLP peers synchronize, then exchange control and data frames.



Layered Transport

Headers for Layers

Application Data

TCP 1480 Total Bytes 20 Bytes 1460 Bytes Payload

IP 1500 Total Bytes 20 Bytes 1480 Bytes Payload

TCP/IP Header Compression

PPP 1470 Total Bytes 4 Bytes 1463 Bytes Payload 3 Bytes

RLP 52 Bytes/Frame 1 2 3 4 5 6 7 8 9 10 ....

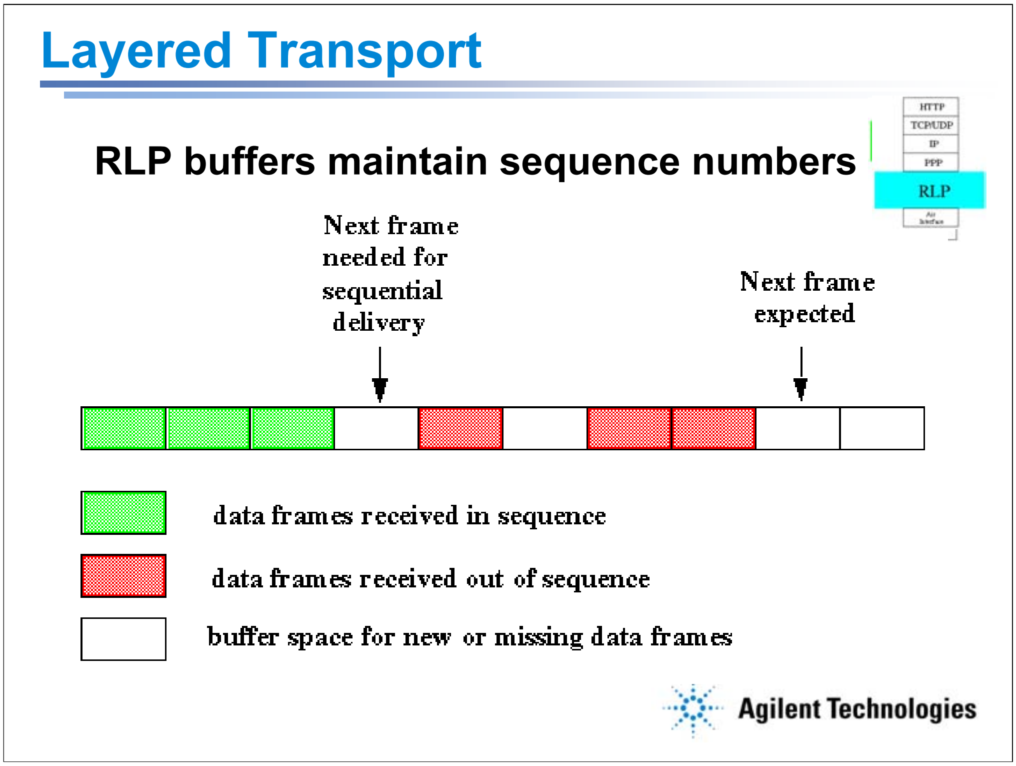
29 Frames

Agilent Technologies

RLP further divides the data sent down from PPP into a frame size suitable for transport over the air interface.

It is expected that RLP frames will be lost over the air interface. In fact, the wireless device’s signal to noise (Eb/Nt) is controlled to a level where the average FER (frame error rate) is often at a level that leaves room for improvement in error rate during periods of exceptionally good RF reception. This makes more efficient use of cell capacity by lowering the average noise interference.

RLP does not care about frame boundaries established by the layer above. RLP simply divides the data up into the size of blocks that is most efficient to stream data from sender to receiver.



Layered Transport

HTTP
TCP/UDP
IP
PPP
RLP
Air Interface

RLP buffers maintain sequence numbers

Next frame needed for sequential delivery

Next frame expected

🟩 data frames received in sequence

🟥 data frames received out of sequence

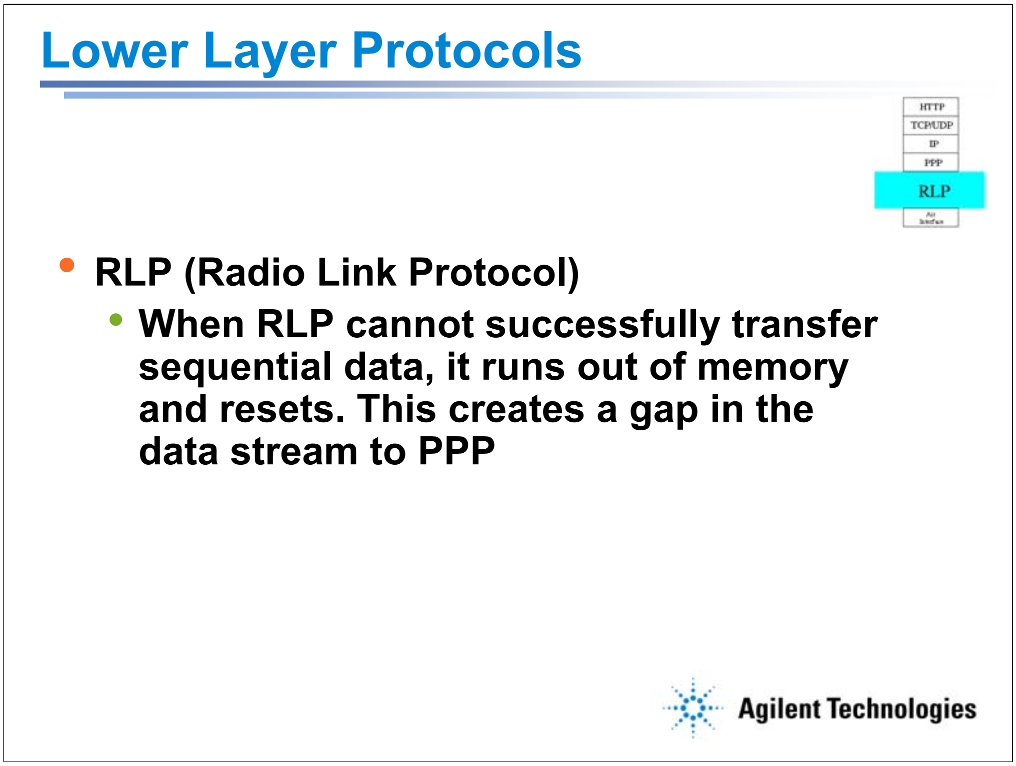
□ buffer space for new or missing data frames

Agilent Technologies

RLP senders and receivers buffer frames of RLP data.

If an RLP frame is received out of sequence, new frames are still received but the receiver lets the sender know that a frame did not arrive in sequence (through a NAK, Negative AcKnowledge).

If the missing frame shows up before storage space runs out, the receiver can put it in the correct sequence and deliver sequential data to PPP. Delivering data to PPP restores buffer space.



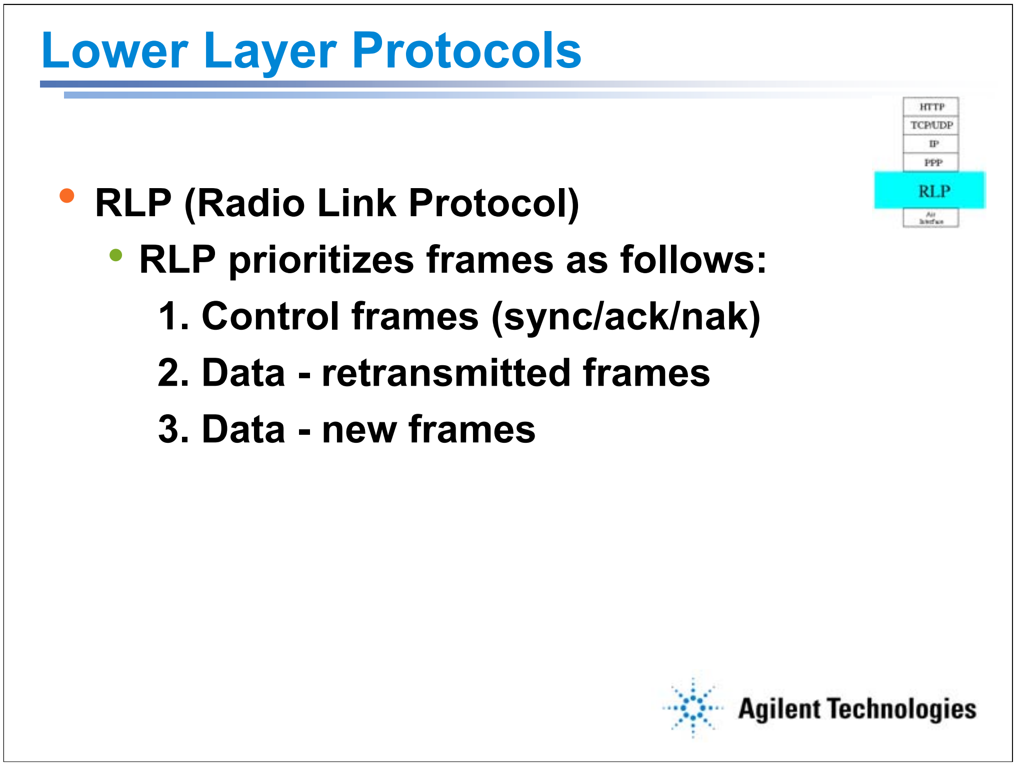
Lower Layer Protocols

HTTP
TCP/UDP
IP
PPP
RLP
Air Interface

- RLP (Radio Link Protocol)
  - When RLP cannot successfully transfer sequential data, it runs out of memory and resets. This creates a gap in the data stream to PPP

Agilent Technologies

If RLP runs out of buffer storage, it performs a reset and flushes memory. All frames not delivered to PPP at this point are lost and it is beyond RLP's ability to recover them.



Lower Layer Protocols

HTTP
TCP/UDP
IP
PPP
RLP
Air Interface

- RLP (Radio Link Protocol)
  - RLP prioritizes frames as follows:
    1. Control frames (sync/ack/nak)
    2. Data - retransmitted frames
    3. Data - new frames

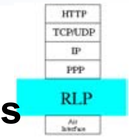
Agilent Technologies

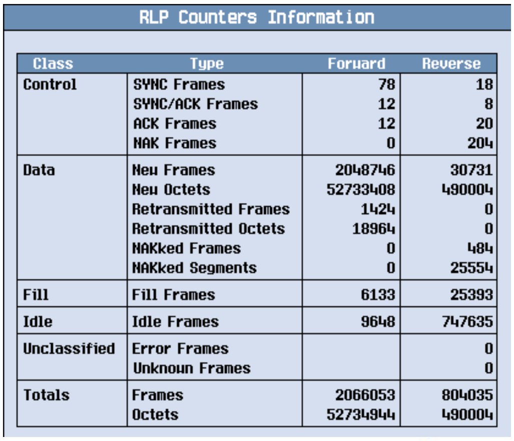
The highest priority frames are the control frames. They are used to synchronize communication and let the sender know when RLP frames need to be retransmitted.

Retransmitted frames have a higher priority than new frames

Lower Layer Protocols

- RLP Counters
  - The test set provides RLP frame counts





RLP Counters Information

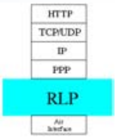
Class	Type	Forward	Reverse
Control	SYNC Frames	78	18
	SYNC/ACK Frames	12	8
	ACK Frames	12	20
	NAK Frames	0	204
Data	New Frames	2048746	30731
	New Octets	52733408	490004
	Retransmitted Frames	1424	0
	Retransmitted Octets	18964	0
	NAKked Frames	0	484
	NAKked Segments	0	25554
Fill	Fill Frames	6133	25393
Idle	Idle Frames	9648	747635
Unclassified	Error Frames		0
	Unknown Frames		0
Totals	Frames	2066053	804035
	Octets	52734944	490004

Agilent Technologies

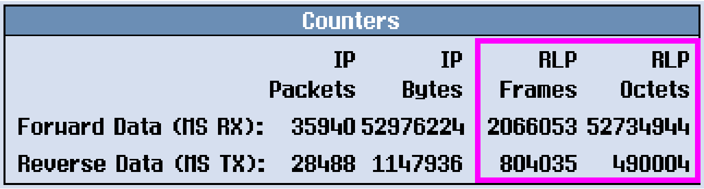
During periods where there is no data passed down from PPP, but the physical air interface is still connected, RLP transmits idle frames.

When data inactivity causes the data connection to go dormant, the physical air interface is disconnected (idle) and the RLP entities stop sending idle frames. The test set will display Idle on the Call Setup Screen.

Lower Layer Protocols

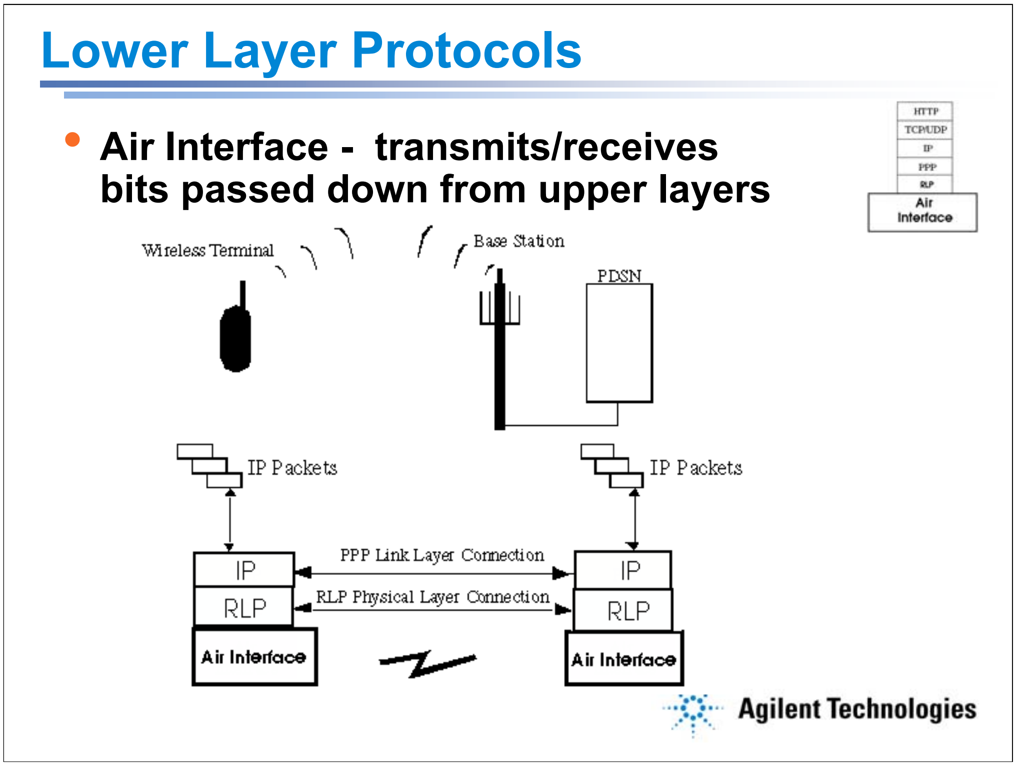


- RLP Summary
  - The test set summarizes IP and RLP frame counts



Counters

	IP Packets	IP Bytes	RLP Frames	RLP Octets
Forward Data (MS RX):	35940	52976224	2066053	52734944
Reverse Data (MS TX):	28488	1147936	804035	490004



Lower Layer Protocols

- Air Interface - transmits/receives bits passed down from upper layers

RLP sends packets down to the air interface where interleaving, coding and modulation is applied to the bits. The physical channel is established as needed, and may include one or more supplemental channels to handle the higher data rates.

The test set sends forward channel data on the fundamental or the fundamental + supplemental channels.

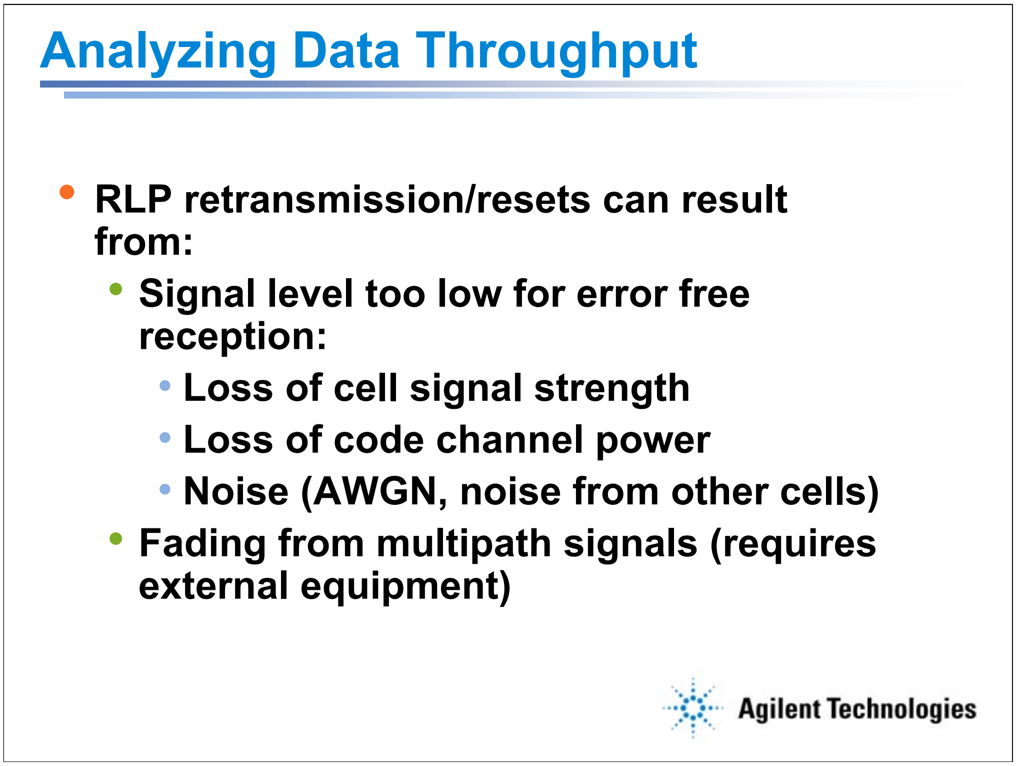
The test set provides controls for varying data rate, RF level, and interference level to simulate the mobile’s environment while on a packet data call.

Error detection and correction at this layer is performed by turbo/convolutional coders.

Agenda

- Introduction
- What is packet switching?
- Network models
- Upper layer (end-to-end) protocols
- Lower layer protocols
- **Analyzing data throughput**

Agilent Technologies



Analyzing Data Throughput

- RLP retransmission/resets can result from:
  - Signal level too low for error free reception:
    - Loss of cell signal strength
    - Loss of code channel power
    - Noise (AWGN, noise from other cells)
  - Fading from multipath signals (requires external equipment)

Agilent Technologies

The coding gain that results from convolutional or turbo encoding at the physical layer provides the first line of defense against data loss due to RF degradation. If the coding gain fails to correct errors, the task of data recovery moves up the protocol stack to RLP.

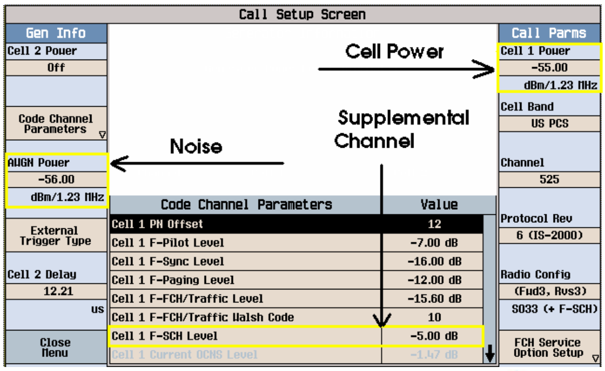
RLP is designed to provide reliable data delivery of PPP frames. The test set can simulate RF degradation and monitor RLP activity.

The test set provides level control of the cell power and level control of a noise generator.

The supplemental channel is also directly settable to a level relative to cell power. Lowering the power level on the forward supplemental channel will eventually interrupt data flow, especially at the higher data rates.

Analyzing Data Throughput

- **Forward channel parameters can induce data errors in a controlled environment**



Call Setup Screen

Cell 2 Power
Off

AWGN Power
-56.00
dBm/1.23 MHz

Cell 2 Delay
12.21
us

Cell 1 Power
-55.00
dBm/1.23 MHz

Cell Band
US PCS

Channel
525

Protocol Rev
6 (IS-2000)

Radio Config
(Fwd3, Rvs3)
SO33 (+ F-SCH)

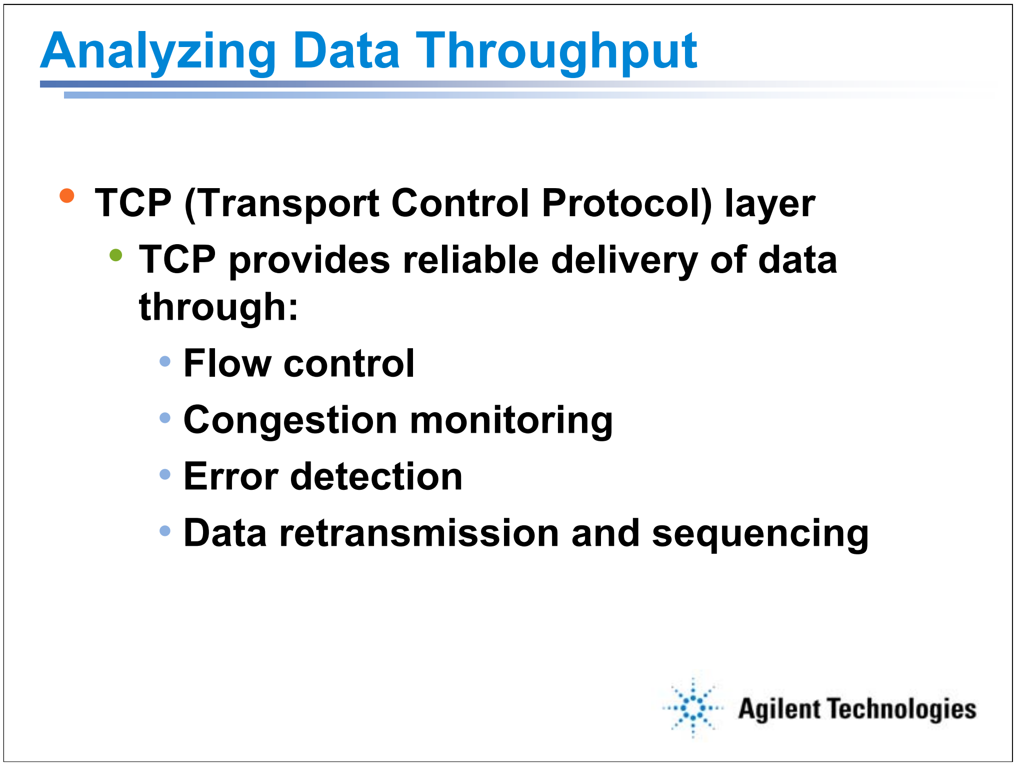
Code Channel Parameters	Value
Cell 1 PN Offset	12
Cell 1 F-Pilot Level	-7.00 dB
Cell 1 F-Sync Level	-16.00 dB
Cell 1 F-Paging Level	-12.00 dB
Cell 1 F-FCH/Traffic Level	-15.60 dB
Cell 1 F-FCH/Traffic Walsh Code	10
Cell 1 F-SCH Level	-5.00 dB
Cell 1 Current OCNS Level	-1.47 dB

Agilent Technologies

The test set provides adjustments to vary relative signal/noise power levels.

This capability can be used to introduce a controlled amount of data loss beginning at the physical channel. The amount of physical channel data loss on the forward supplemental channel can be measured by bringing up a call in service option 32, which is a data loopback service option, and measuring TDSO FER. A description of this measurement is beyond the scope of this paper but can be found by going to the Agilent.comwebsite and searching on TDSO FER.

Eventually, RLP retransmissions will occur, then RLP resets. At this point, TCP retransmission will occur because all layers below it have failed to deliver data sequentially.

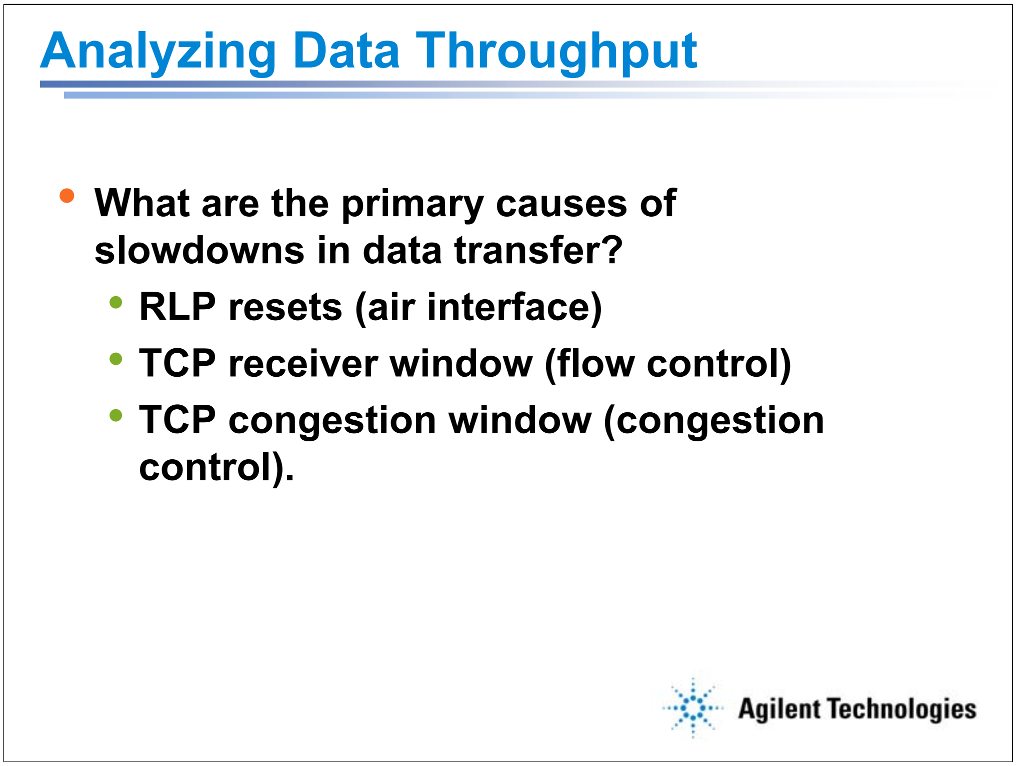


Analyzing Data Throughput

- TCP (Transport Control Protocol) layer
  - TCP provides reliable delivery of data through:
    - Flow control
    - Congestion monitoring
    - Error detection
    - Data retransmission and sequencing

Agilent Technologies

Let’s turn our attention back to the TCP layer. Since this is the layer that is ultimately responsible for delivery of data to/from the application layer, monitoring TCP gives valuable information about network performance.



Analyzing Data Throughput

- What are the primary causes of slowdowns in data transfer?
  - RLP resets (air interface)
  - TCP receiver window (flow control)
  - TCP congestion window (congestion control).

Agilent Technologies

The areas of interest when analyzing the effects of lost data are:

RLP - if the circular buffer is overrun it performs a reset.

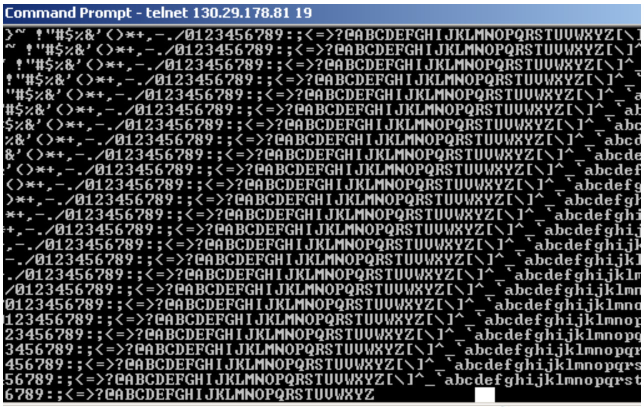
TCP receiver window - receiver runs out of buffer space

TCP congestion window - TCP senses what it thinks is network congestion and slows down.

.

Analyzing Data Throughput

- Data sources
  - FTP
  - Download video or graphics
  - TELNET <IP Address> 19



```
}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]
~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`a
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ab
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcd
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcde
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdef
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
/0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
23456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
3456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
56789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
6789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

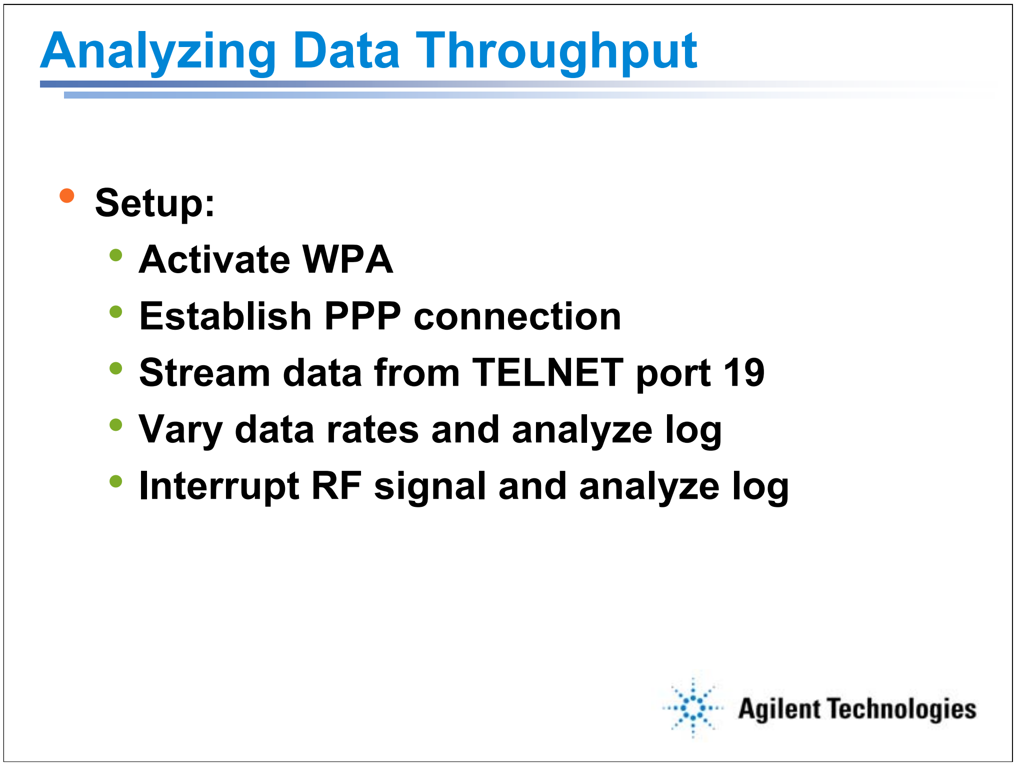
Agilent Technologies

To observe date throughput a significant amount of data must be sent to the wireless device.

CDG Stage two testing specifies a file that can be sent to the wireless device using the FTP protocol. Some video streaming files or graphics files also provide adequate data.

For this demonstration, a laptop PC was used to request a TELNET connection with a UNIX computer. The wireless device was a phone functioning as a modem.

One of the protocol ports available through TELNET is port 19, which sends a stream of alphanumeric characters until the session is ended by the user. The characters are displayed in a window and make it easy to see when data flow increases or decreases.



Analyzing Data Throughput

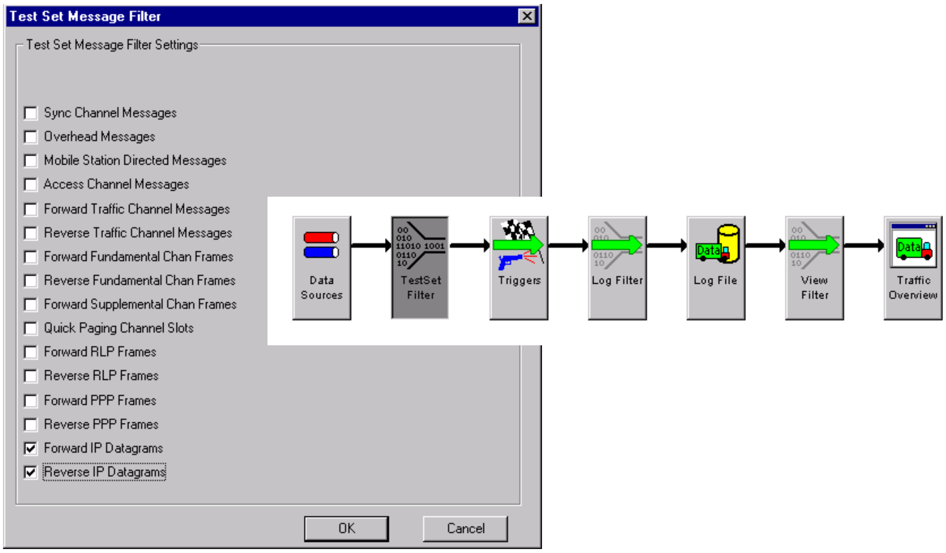
- Setup:
  - Activate WPA
  - Establish PPP connection
  - Stream data from TELNET port 19
  - Vary data rates and analyze log
  - Interrupt RF signal and analyze log

Agilent Technologies

A TCP connection to TELNET port 19, which is available on all unix machines will provide a visual means of monitoring the flow of data to the device that requests this port.

Transmitted characters will automatically scroll across the command prompt window.

Analyzing Data Throughput



Test Set Message Filter

Test Set Message Filter Settings

- □ Sync Channel Messages
- □ Overhead Messages
- □ Mobile Station Directed Messages
- □ Access Channel Messages
- □ Forward Traffic Channel Messages
- □ Reverse Traffic Channel Messages
- □ Forward Fundamental Chan Frames
- □ Reverse Fundamental Chan Frames
- □ Forward Supplemental Chan Frames
- □ Quick Paging Channel Slots
- □ Forward RLP Frames
- □ Reverse RLP Frames
- □ Forward PPP Frames
- □ Reverse PPP Frames
- ☑ Forward IP Datagrams
- ☑ Reverse IP Datagrams

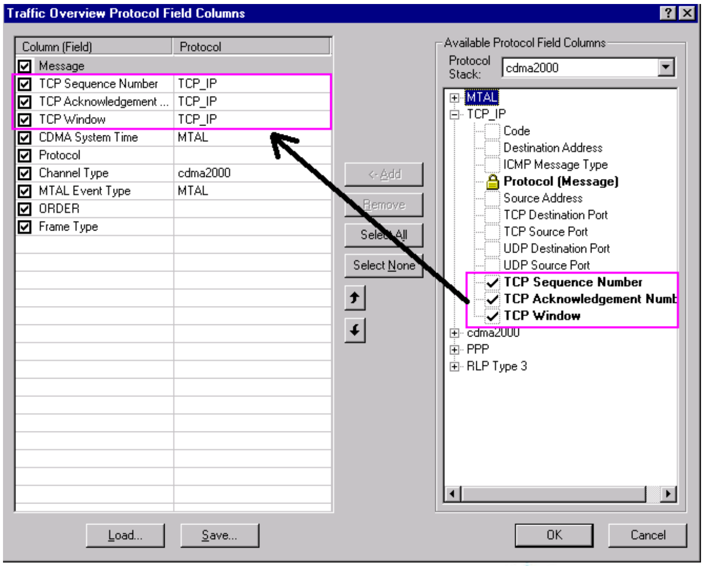
OK Cancel

Agilent Technologies

The Test Set Message Filter allows filtering messages that are sent to the WPA software. In this setup, we are only interested in the Forward and Reverse IP Datagrams, which carry encapsulated TCP segments, so these boxes are checked.

Filtering can also be performed at the Log Filter and View Filters stages.

Analyzing Data Throughput



Traffic Overview Protocol Field Columns

Column (Field)	Protocol
☑ Message	
☑ TCP Sequence Number	TCP_IP
☑ TCP Acknowledgement ...	TCP_IP
☑ TCP Window	TCP_IP
☑ CDMA System Time	MTAL
☑ Protocol	
☑ Channel Type	cdma2000
☑ MTAL Event Type	MTAL
☑ ORDER	
☑ Frame Type	

Available Protocol Field Columns

Protocol Stack: cdma2000

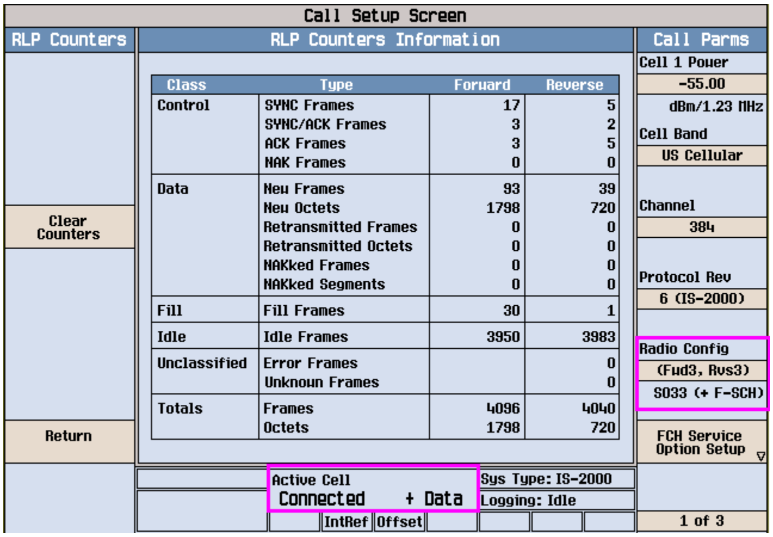
- MTAL
- TCP_IP
  - Code
  - Destination Address
  - ICMP Message Type
  - **Protocol (Message)**
  - Source Address
  - TCP Destination Port
  - TCP Source Port
  - UDP Destination Port
  - UDP Source Port
  - ✓ **TCP Sequence Number**
  - ✓ **TCP Acknowledgement Numb**
  - ✓ **TCP Window**
- cdma2000
- PPP
- RLP Type 3

Agilent Technologies

The WPA allows customization of columns displayed in the Traffic Overview window. Since we are interested in analyzing TCP_IP protocol, we will select three fields that the sender and receiver use to control the rate of data flow at the TCP layer.

The window on the right selects the message fields of interest and the window on the left specifies which column they will be displayed in.

Analyzing Data Throughput



Call Setup Screen

RLP Counters

Clear Counters

Return

RLP Counters Information

Class	Type	Forward	Reverse
Control	SYNC Frames	17	5
	SYNC/ACK Frames	3	2
	ACK Frames	3	5
	NAK Frames	0	0
Data	New Frames	93	39
	New Octets	1798	720
	Retransmitted Frames	0	0
	Retransmitted Octets	0	0
	NAKked Frames	0	0
	NAKked Segments	0	0
Fill	Fill Frames	30	1
Idle	Idle Frames	3950	3983
Unclassified	Error Frames		0
	Unknown Frames		0
Totals	Frames	4096	4040
	Octets	1798	720

Call Parms

Cell 1 Power
-55.00
dBm/1.23 MHz

Cell Band
US Cellular

Channel
384

Protocol Rev
6 (IS-2000)

Radio Config
(Fwd3, Rvs3)
SO33 (+ F-SCH)

FCH Service Option Setup

Active Cell
Connected + Data

Sys Type: IS-2000
Logging: Idle

IntRef Offset

1 of 3

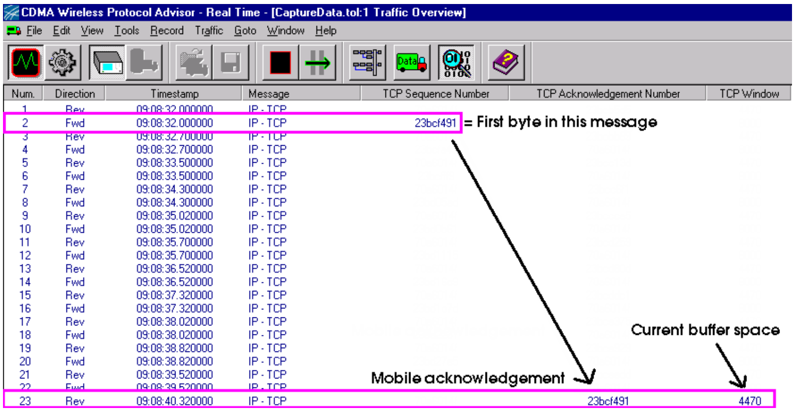
Agilent Technologies

When a service is requested, whether it be TELNET port 19, requesting a web page using HTTP protocol, or initiating the transfer of a file using FTP, a PPP connection must be established and the physical channel resources allocated to permit data transfer over the air interface.

The test set displays Connected +Data when a service option 33 call is connected. If data transfer is stopped for a long enough period of time, the test set will display Idle, indicating the physical channel has been released. The PPP connection may remain, however, so that the PPP connection setup does not have to be repeated the next time data is requested.

Analyzing Data Throughput

- **TCP Sequence numbering - 9600 bps**



CDMA Wireless Protocol Advisor - Real Time - [CaptureData.tol:1 Traffic Overview]
File Edit View Tools Record Traffic Goto Window Help

Num.	Direction	Timestamp	Message	TCP Sequence Number	TCP Acknowledgement Number	TCP Window
1	Rev	09:08:32.000000	IP - TCP			
2	Fwd	09:08:32.000000	IP - TCP	23bcf491		
3	Rev	09:08:32.700000	IP - TCP			
4	Fwd	09:08:32.700000	IP - TCP			
5	Rev	09:08:33.500000	IP - TCP			
6	Fwd	09:08:33.500000	IP - TCP			
7	Rev	09:08:34.300000	IP - TCP			
8	Fwd	09:08:34.300000	IP - TCP			
9	Rev	09:08:35.020000	IP - TCP			
10	Fwd	09:08:35.020000	IP - TCP			
11	Rev	09:08:35.700000	IP - TCP			
12	Fwd	09:08:35.700000	IP - TCP			
13	Rev	09:08:36.520000	IP - TCP			
14	Fwd	09:08:36.520000	IP - TCP			
15	Rev	09:08:37.320000	IP - TCP			
16	Fwd	09:08:37.320000	IP - TCP			
17	Rev	09:08:38.020000	IP - TCP			
18	Fwd	09:08:38.020000	IP - TCP			
19	Rev	09:08:38.820000	IP - TCP			
20	Fwd	09:08:38.820000	IP - TCP			
21	Rev	09:08:39.520000	IP - TCP			
22	Fwd	09:08:39.520000	IP - TCP			
23	Rev	09:08:40.320000	IP - TCP		23bcf491	4470

= First byte in this message

Current buffer space

Mobile acknowledgement

Agilent Technologies

This display was generated by sending data to the mobile at 9.6 kbps using TELNET port 19. WPA Test Set Message Filter Settings was set to include Forward and Reverse IP Datagrams only. This representation of the WPA display has been altered to highlight areas of particular interest.

Note that the pattern here is alternating between forward and reverse channel messages. Forward channel messages are occurring a little more frequently than one per second.

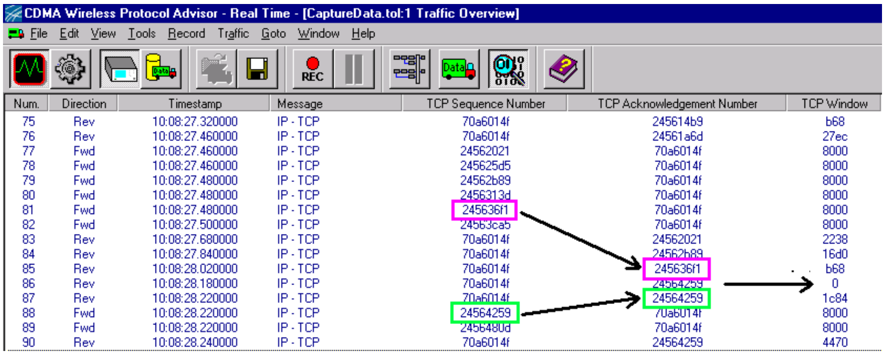
No data is being sent on the reverse channel.

The first message shows a Fwd (forward) TCP Sequence Number of 1bb48f23. The TCP Sequence Number identifies the first byte of data in this segment being sent .

Eight seconds later, the reverse channel (mobile) sent a message acknowledging that it had received all bytes up to 1bb48f23. The mobile also let the sender know that it has 4470 bytes of buffer space in the TCP Window field, which was max for this phone.

Analyzing Data Throughput

- **TCP Sequence numbering - 153.6 kbps**


CDMA Wireless Protocol Advisor - Real Time - [CaptureData.tol:1 Traffic Overview]
File Edit View Tools Record Traffic Goto Window Help
REC
Data

Num.	Direction	Timestamp	Message	TCP Sequence Number	TCP Acknowledgement Number	TCP Window
75	Rev	10:08:27.320000	IP - TCP	70a6014f	245614b9	b68
76	Rev	10:08:27.460000	IP - TCP	70a6014f	24561a6d	27ec
77	Fwd	10:08:27.460000	IP - TCP	24562021	70a6014f	8000
78	Fwd	10:08:27.460000	IP - TCP	245625d5	70a6014f	8000
79	Fwd	10:08:27.480000	IP - TCP	24562b89	70a6014f	8000
80	Fwd	10:08:27.480000	IP - TCP	2456313d	70a6014f	8000
81	Fwd	10:08:27.480000	IP - TCP	245636f1	70a6014f	8000
82	Fwd	10:08:27.500000	IP - TCP	24563ca5	70a6014f	8000
83	Rev	10:08:27.680000	IP - TCP	70a6014f	24562021	2238
84	Rev	10:08:27.840000	IP - TCP	70a6014f	24562b89	16d0
85	Rev	10:08:28.020000	IP - TCP	70a6014f	245636f1	b68
86	Rev	10:08:28.180000	IP - TCP	70a6014f	24564259	0
87	Rev	10:08:28.220000	IP - TCP	70a6014f	24564259	1c84
88	Fwd	10:08:28.220000	IP - TCP	24564259	70a6014f	8000
89	Fwd	10:08:28.220000	IP - TCP	2456480d	70a6014f	8000
90	Rev	10:08:28.240000	IP - TCP	70a6014f	24564259	4470

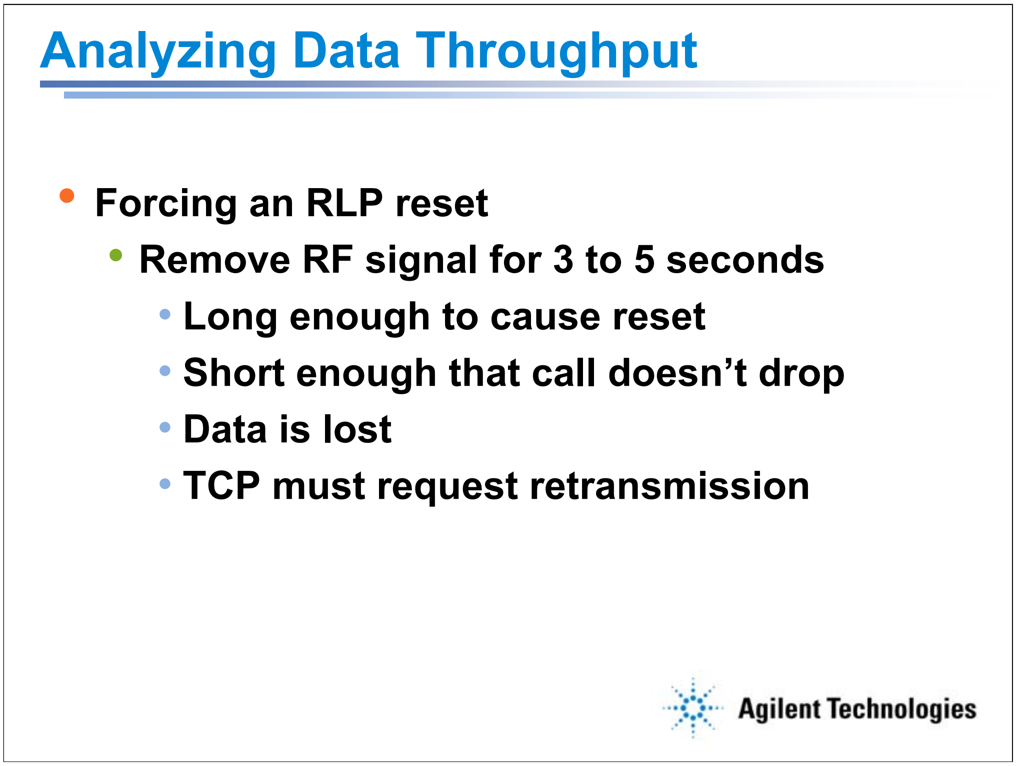
Agilent Technologies

In this display, the data rate has been increased to 153.6 kbps.

Notice that the number of messages per second has greatly increased. Now forward channel messages are occurring at a rate of approximately eight per second. The mobile is reacting much faster in sending acknowledgements.

Also, notice that in message 86 the TCP Window shrunk to 0, prompting the TCP sender to slow down. The message from the mobile station highlighted in line 87 shows that the TCP Acknowledgement Number did not increment due to the TCP Window going to zero in message 86. The mobile is still asking for data beginning at 24564259 but indicates it now has buffer space.

The sending TCP has held off sending this segment of data and ends up sending it in line 88.



Analyzing Data Throughput

- Forcing an RLP reset
  - Remove RF signal for 3 to 5 seconds
    - Long enough to cause reset
    - Short enough that call doesn’t drop
    - Data is lost
    - TCP must request retransmission

Agilent Technologies

When data is lost over the air interface, RLP will send NAKs (negative acknowledgements) to the sender and will have the frames retransmitted. This will work up to a point. Due to limits on buffer space RLP will perform a reset if its ability to recover lost data cannot keep up with the rate of data loss. At this point, the job of recovering lost data gets pushed to the upper layer protocol TCP.

To force an RLP reset, open the RF path to the wireless device for a period of 3 to 5 seconds. This will be long enough to force a RLP reset, but not long enough to drop the call. For reference information, this is the technique used in:

CDG Stage 2 Interoperability Tests

(TIA/EIA/IS-2000)

March 26, 2001

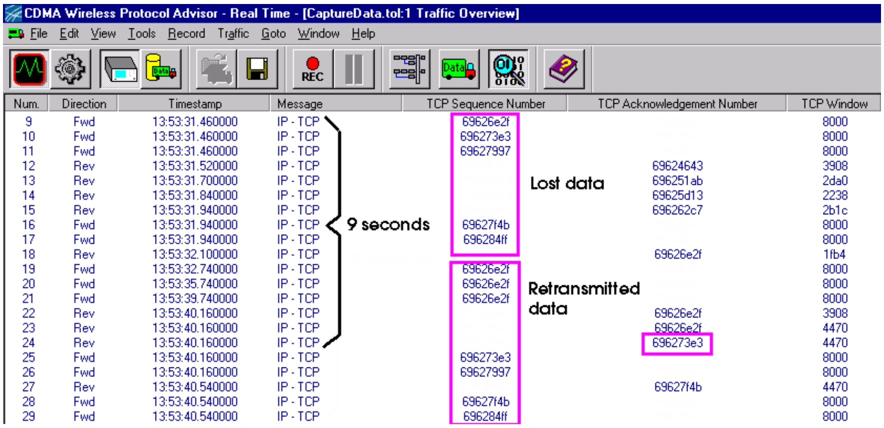
Revision 1.0

CDG 57

10.1.12 RLP Abort and TCP Retransmit Test

Analyzing Data Throughput

- **TCP Retransmission**



CDMA Wireless Protocol Advisor - Real Time - [CaptureData.tol:1 Traffic Overview]
File Edit View Tools Record Traffic Goto Window Help
REC

Num.	Direction	Timestamp	Message	TCP Sequence Number	TCP Acknowledgement Number	TCP Window
9	Fwd	13:53:31.460000	IP - TCP	69626e2f		8000
10	Fwd	13:53:31.460000	IP - TCP	696273e3		8000
11	Fwd	13:53:31.460000	IP - TCP	69627997		8000
12	Rev	13:53:31.520000	IP - TCP		69624643	3908
13	Rev	13:53:31.700000	IP - TCP		696251ab	2da0
14	Rev	13:53:31.840000	IP - TCP		69625d13	2238
15	Rev	13:53:31.940000	IP - TCP		696262c7	2b1c
16	Fwd	13:53:31.940000	IP - TCP	69627f4b		8000
17	Fwd	13:53:31.940000	IP - TCP	696284ff		8000
18	Rev	13:53:32.100000	IP - TCP		69626e2f	1fb4
19	Fwd	13:53:32.740000	IP - TCP	69626e2f		8000
20	Fwd	13:53:35.740000	IP - TCP	69626e2f		8000
21	Fwd	13:53:39.740000	IP - TCP	69626e2f		8000
22	Rev	13:53:40.160000	IP - TCP		69626e2f	3908
23	Rev	13:53:40.160000	IP - TCP		69626e2f	4470
24	Rev	13:53:40.160000	IP - TCP		696273e3	4470
25	Fwd	13:53:40.160000	IP - TCP	696273e3		8000
26	Fwd	13:53:40.160000	IP - TCP	69627997		8000
27	Rev	13:53:40.540000	IP - TCP		69627f4b	4470
28	Fwd	13:53:40.540000	IP - TCP	69627f4b		8000
29	Fwd	13:53:40.540000	IP - TCP	696284ff		8000

9 seconds

Lost data

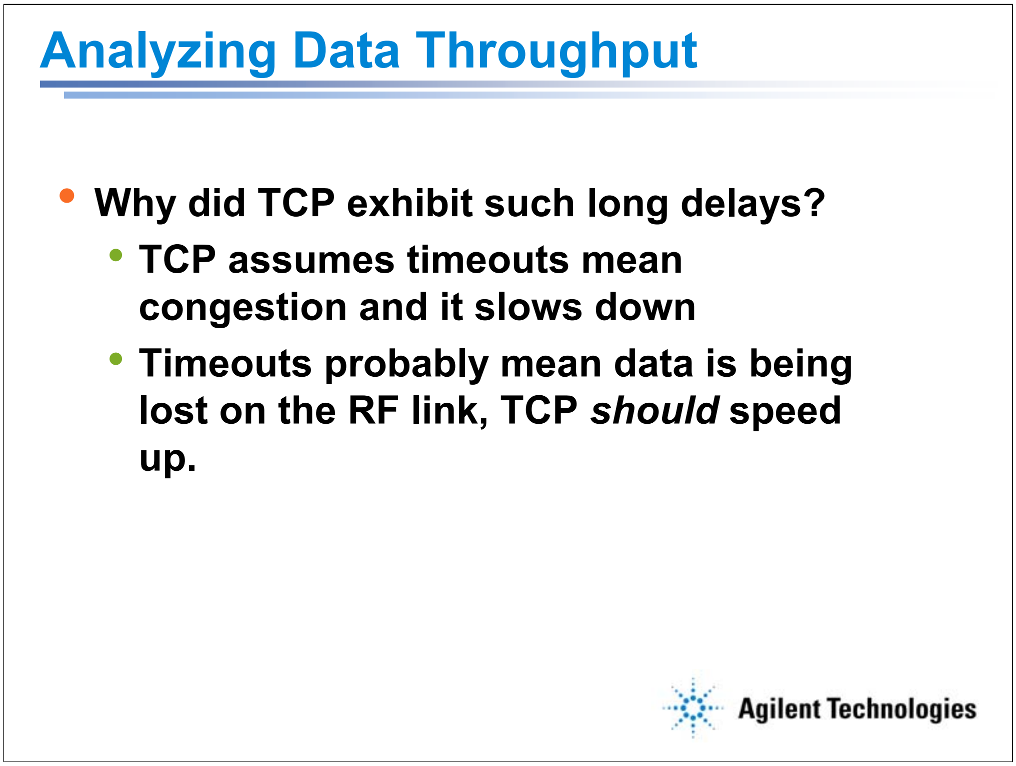
Retransmitted data

Agilent Technologies

In this display the RF path to the mobile was removed for 3 seconds. RLP does not buffer enough data to handle the interruption so the TCP layer has to retransmit lost segments.

The data in the first message in this display, message 9, begins at 69626e2f. In message 23 the mobile station acknowledges receiving all data before 69626e2f, but it is not until message 24 that the mobile station indicates it received data beyond 69626e2f. The process of retransmitting lost TCP segments took over 9 seconds.

After message 24, the forward channel retransmitted the next four 1500 byte segments.



Analyzing Data Throughput

- **Why did TCP exhibit such long delays?**
  - **TCP assumes timeouts mean congestion and it slows down**
  - **Timeouts probably mean data is being lost on the RF link, TCP *should* speed up.**

Agilent Technologies

When the RF path was disconnected, RLP did not have enough buffer space to fill the gap, so it reset. When the TCP sender's retransmission timer timed out, it assumed that there was congestion in the network and adjusted its congestion window, which determines how large a burst of data it can send, to let network traffic clear up.

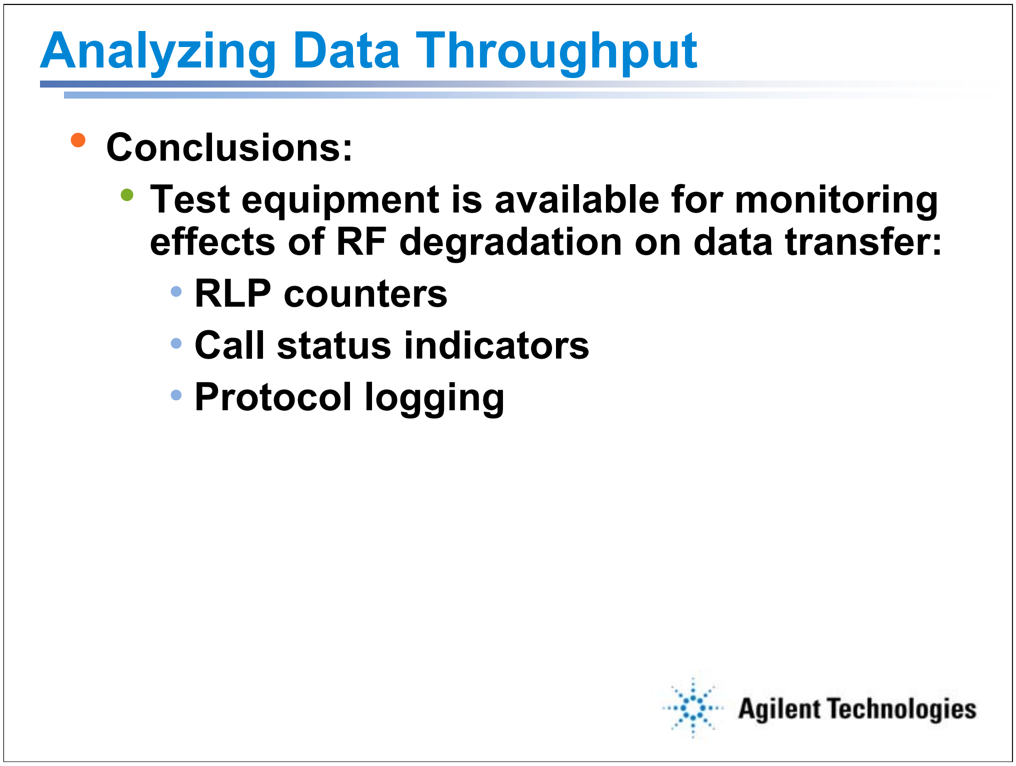
Messages 20 and 21 were only one-segment bursts, delayed 3 and 4 seconds respectively. No messages from the mobile station were received during this time.

After acknowledgments resume, the TCP receiver will gradually increase the congestion window up again until another timeouts or the receiver TCP window says its buffers are full.

Since the data loss was caused by disruption to the RF signal, not network congestion or receiver buffer overflow, it would be better for throughput if TCP would speed up. This is an inefficiency in networks that include an RF subnet that is caused by the TCP congestion algorithm.

Analyzing Data Throughput

- Conclusions:
  - The wireless portion of the network is inherently unreliable.
  - TCP/IP is not designed to handle data loss due to RF degradation.
  - It is important to test end user applications during data slowdowns.



Analyzing Data Throughput

- Conclusions:
  - Test equipment is available for monitoring effects of RF degradation on data transfer:
    - RLP counters
    - Call status indicators
    - Protocol logging

Agilent Technologies

RLP counters to to see if retransmissions are happening

Call status indicator to see if a call has been dropped.

Protocol logging to monitor specific layers of protocol during RF degradation.