



# Troubleshooting IP Telephony Networks - Case Studies



**Peter Leung**

# Session Objectives

- **Analysis and troubleshoot some real world problems**
- Understand how to trace the call flow of a call from the call manager traces and identify the important information
- Understand how to use various built-in and external troubleshooting tools to assist in data gathering and analysis
- Use collected data to find root cause of some real-world problems

# What You Should Know

- Cisco CallManager configuration and operation
- Cisco IOS® voice gateway configuration and operation
- Use of Network Sniffer
- Basic understanding of:
  - Skinn Client Control Protocol (SCCP)
  - H.323



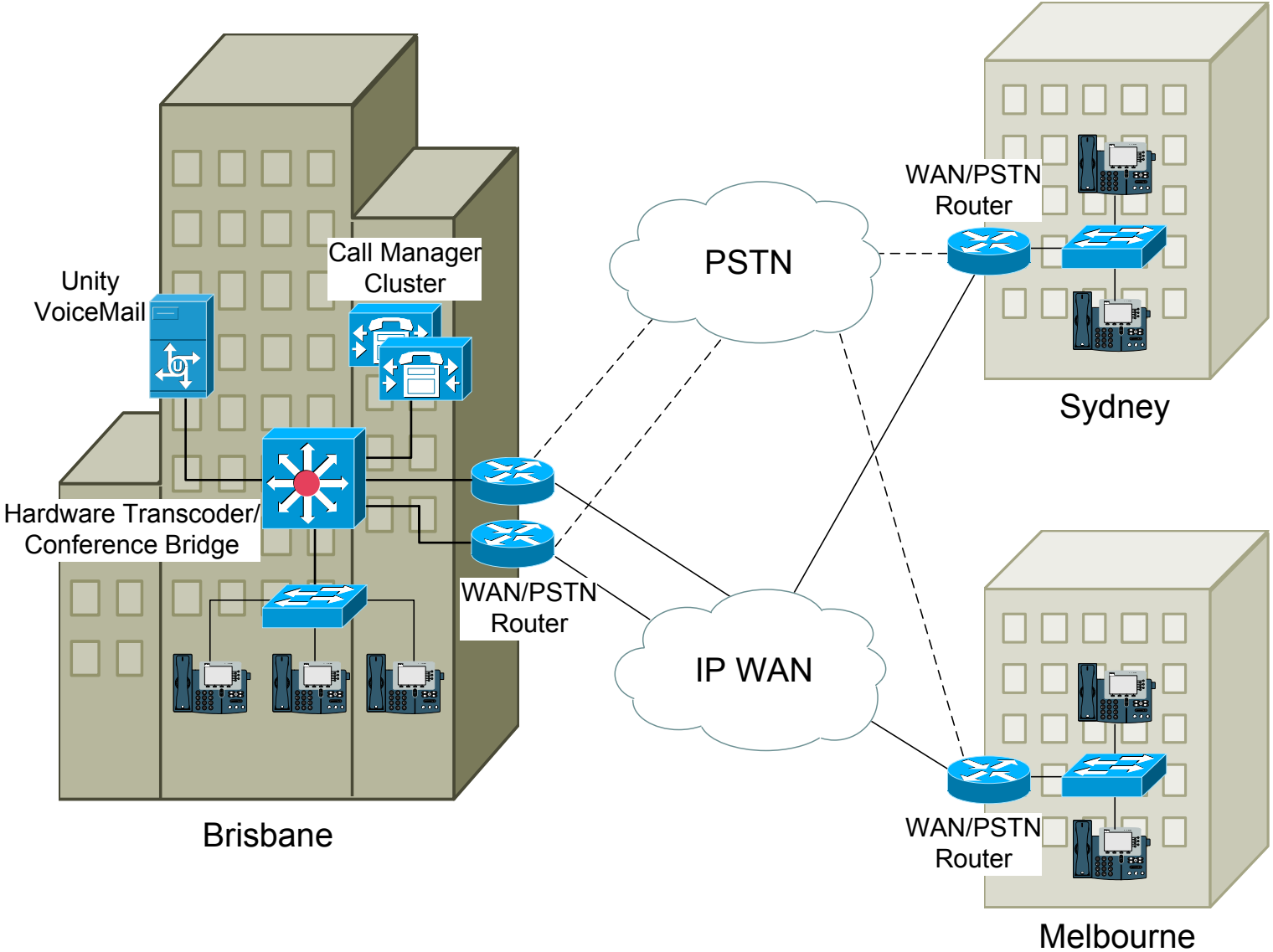
# Agenda

- Introduction
- Company Network Overview
- Case Study 1: Dropped Call
- Case Study 2: Intermittent voice quality issue

# Agenda

- Introduction
- **Company Network Overview**
- Case Study 1: Dropped Call
- Case Study 2: Intermittent voice quality issue

# Company Network Overview



# Agenda

- Introduction
- Company Network Overview
- Case Study 1: Dropped Call
- Case Study 2: Intermittent voice quality issue

# Case Study 1: Dropped Call

“Hello Pete, need your help! A user has reported that while she was on the phone with a customer, the call dropped for no reason”





# Questions to Ask

## Questions to Ask About “A User’s Call Was Dropped”

- Who was the user?  
**Simon Barker**
- What is the directory number on their phone?  
**2303**
- What is the MAC address of their phone?  
**SEP0002FD3BAF0B**
- What time did the dropped call occur?  
**Around 03:07 p.m. on August 10**



## Questions to Ask (Contd..)

- Who was the user speaking on the call that was dropped (internal vs. external)?
  - External; Phone number 0401252111
- Was the call inbound or outbound?
  - Inbound
- What was the duration of the call?
  - About two minutes before the call was dropped

# Problem Description

## Formulate a Problem Description

Simon Barker received a call around 03:07 p.m. on August 10, 2006 from 0401252111.

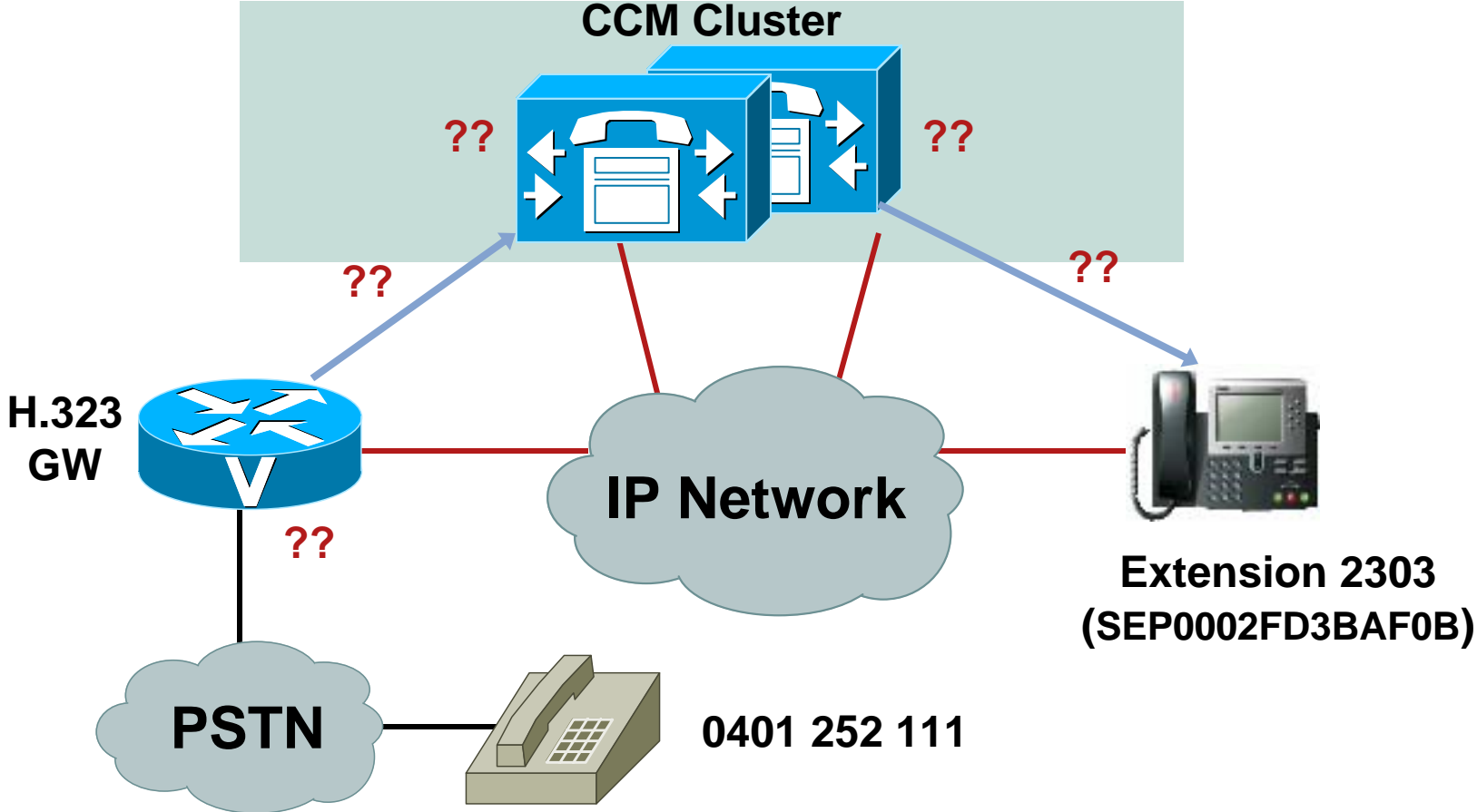
He received the call on extension 2303 on the phone identified as SEP0002FD3BAF0B.

About two minutes into the call, the call was dropped.

# Action Plan

- **Identify and complete the call flow diagram**
- **Locate the disconnect reason**
- **Determine the device sending the disconnect.**
- **Investigate the root cause of the disconnect**

# Call Flow Diagram



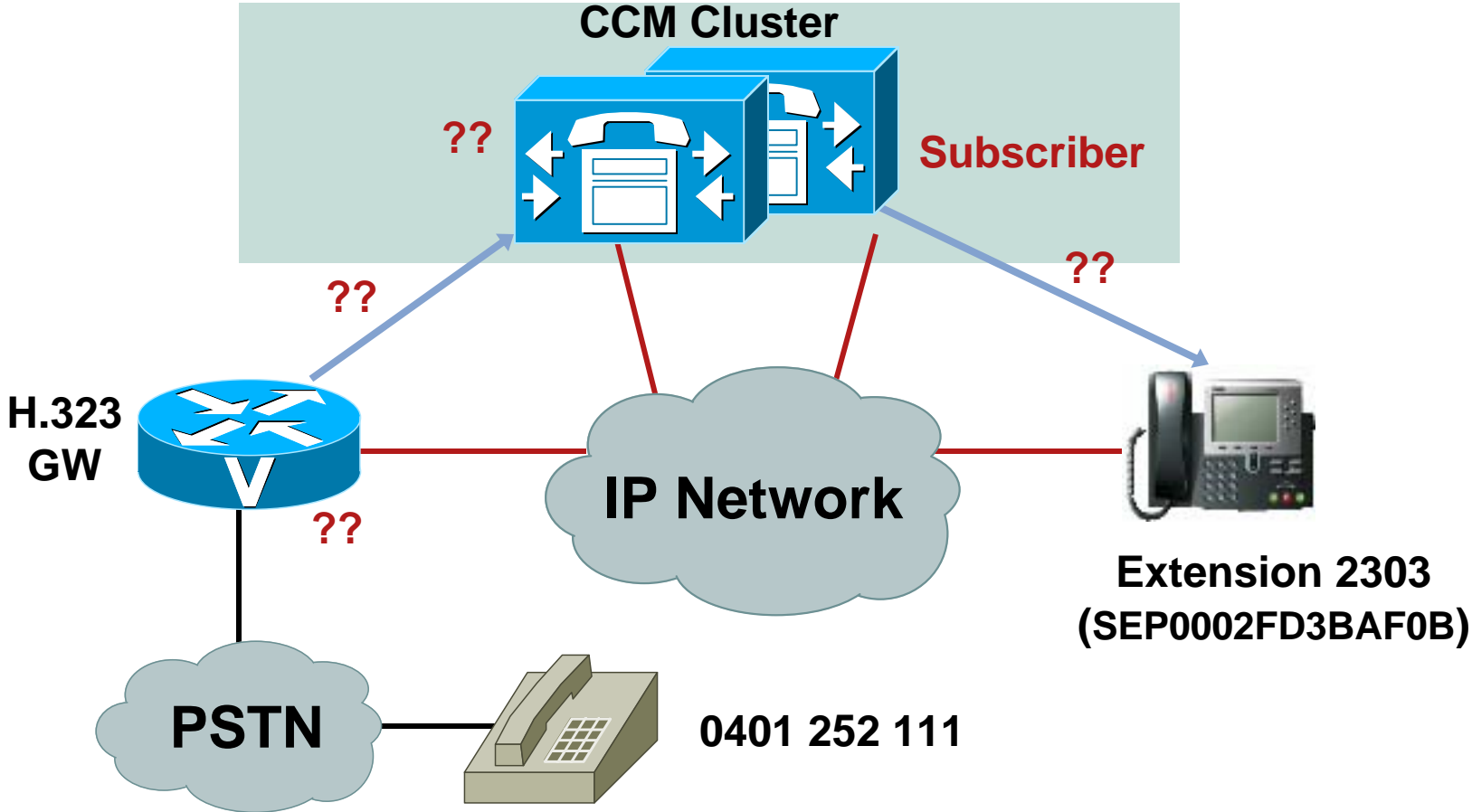
# Phone Registration

The screenshot displays the Cisco Unified CallManager Administration web interface. At the top, a navigation menu includes System, Route Plan, Service, Feature, Device, User, Application, and Help. The main header reads "Cisco Unified CallManager Administration" with the tagline "For Cisco Unified Communications" and the Cisco Systems logo. The page title is "Phone Configuration". On the right side, there are several links: "Add a new phone", "Add/Update Speed Dials", "Add/Update Busy Lamp Fields", "Subscribe/Unsubscribe Services", "Dependency Records", and "Back to Find/List Phones".

The main content area is divided into two columns. The left column contains a sidebar with "Directory Numbers" and "Base Phone" sections. Under "Base Phone", there are two entries: "Line 1 - 2303 (no Partition)" and "Line 2 - Add new DN". The right column displays the configuration for a specific phone: "Phone: SEP0002FD3BAF0B (Auto 3001)", "Registration: Registered with Cisco CallManager 10.66.88.11", and "IP Address: 10.66.6.204". The status is "Ready". Below this information are four buttons: "Copy", "Update", "Delete", and "Reset Phone".

Below the buttons is a section titled "Phone Configuration (Model = Cisco 7960)" and "Device Information". This section contains three input fields: "MAC Address\*" with the value "0002FD3BAF0B", "Description" with the value "Auto 3001", and "Owner User ID" with a dropdown menu showing "(Select User ID)".

# Call Flow Diagram



# Trace Collection Tool

## Various Ways to Collect Trace Files:

- Map a share to the server
- Use the Trace Collection Tool introduced in Cisco CallManager 4.0

Download from **Cisco CallManager Administration > Applications > Plugins**



# Trace Collection Tool

**Cisco CallManager Trace Collection Tool**

Help

**Provide CallManager Details**

Server Name/IP Address: 172.18.106.58

User Name: administrator

Password: xxxxxxxx

To Collect Traces:

- Use IP Address(Convert DNS Names of CallManager Servers to IP Addresses)
- Use DNS Names(Convert IP Addresses of CallManager Servers to DNS Names)

Secure Connection

< Back      Next >

---

**Cisco CallManager Trace Collection Tool**

Help View

**Select CallManager Services or CallManager Applications or System Traces**

Select CallManager Services | Select CallManager Applications | Select System Traces

Select all Services on all Servers

Services	172.18.106.58	172.18.106.59
Cisco CallManager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Tftp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Messaging Interface	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco IP Voice Media Streaming App	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco CTIManager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Telephony Call Dispatcher	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco MOH Audio Translator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco RIS Data Collector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Extension Mobility	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Database Layer Monitor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco CDR Insert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco IP Manager Assistant	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Extended Functions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

< Back      Next >      Exit

# Trace Collection Tool

The screenshot shows the 'Cisco CallManager Trace Collection Tool' window. It has a menu bar with 'Help' and 'View'. The main area is titled 'Collect Traces' and contains a radio button for 'Collect All Available Traces'. Below this is a 'Date Range' section with a radio button for 'Traces for a Date Range'. This section includes a 'Select Time Zone' dropdown menu set to '(GMT-05:00) Eastern Time (US & Can)', a 'Show Server Time Zones' button, 'From Time' and 'To Time' fields with date and time pickers. A note below these fields explains that the display format depends on machine settings. At the bottom of the 'Date Range' section is a 'Zip File Location' text box containing 'C:\CiscoCallManagerTraceCollection.zip' and a browse button. Below that are 'Create Multi Volume Zip File when Zipping' (checkbox), 'MultiVolume File Size' (spinner set to 100 KB), and 'Compression Factor' (dropdown set to '5 - Medium'). At the very bottom are three buttons: '<Back', 'Collect Traces', and 'Exit'.

- Time/Date Range
- Zip Compression

# Finding the Dropped Call

How Do We Find This Call in the Trace Files? Our Three Options Are:

- Search for everything that happened on device SEP0002FD3BAF0B at the time of the problem
- Search for calls to extension 2303
- Search for calls from 0401252111

# Finding the Dropped Call

- We will be searching through the Cisco CallManager CCM (SDI) trace files

Located in C:\Program Files\Cisco\Trace\CCM

- We will use SDL trace files to help us correlate some of the information in the CCM trace files

Located in C:\Program Files\Cisco\Trace\SDL\CCM

# Example - SCCP Trace Data

## SCCP Trace Data in a CCM Trace

08/08/2006 09:37:31.240 CCM|StationInit: (0002129) OffHook.|  
<CLID::StandAloneCluster><NID::10.66.88.11><CT::2,100,124,1.348485>  
<IP::10.66.6.204><DEV::SEP0002FD3BAF0B>

Field Name	Description
Date and Time	Date and Time the event occurred
SCCP Message Direction	StationInit = SCCP Device → Cisco CallManager StationD = Cisco CallManager → SCCP Device
TCP Handle	Unique identifier for a device registered to a Cisco CallManager
SCCP Message Data	SCCP message and all data fields sent as part of that message
XML Trace Data	Extra data used by some tools that you should ignore

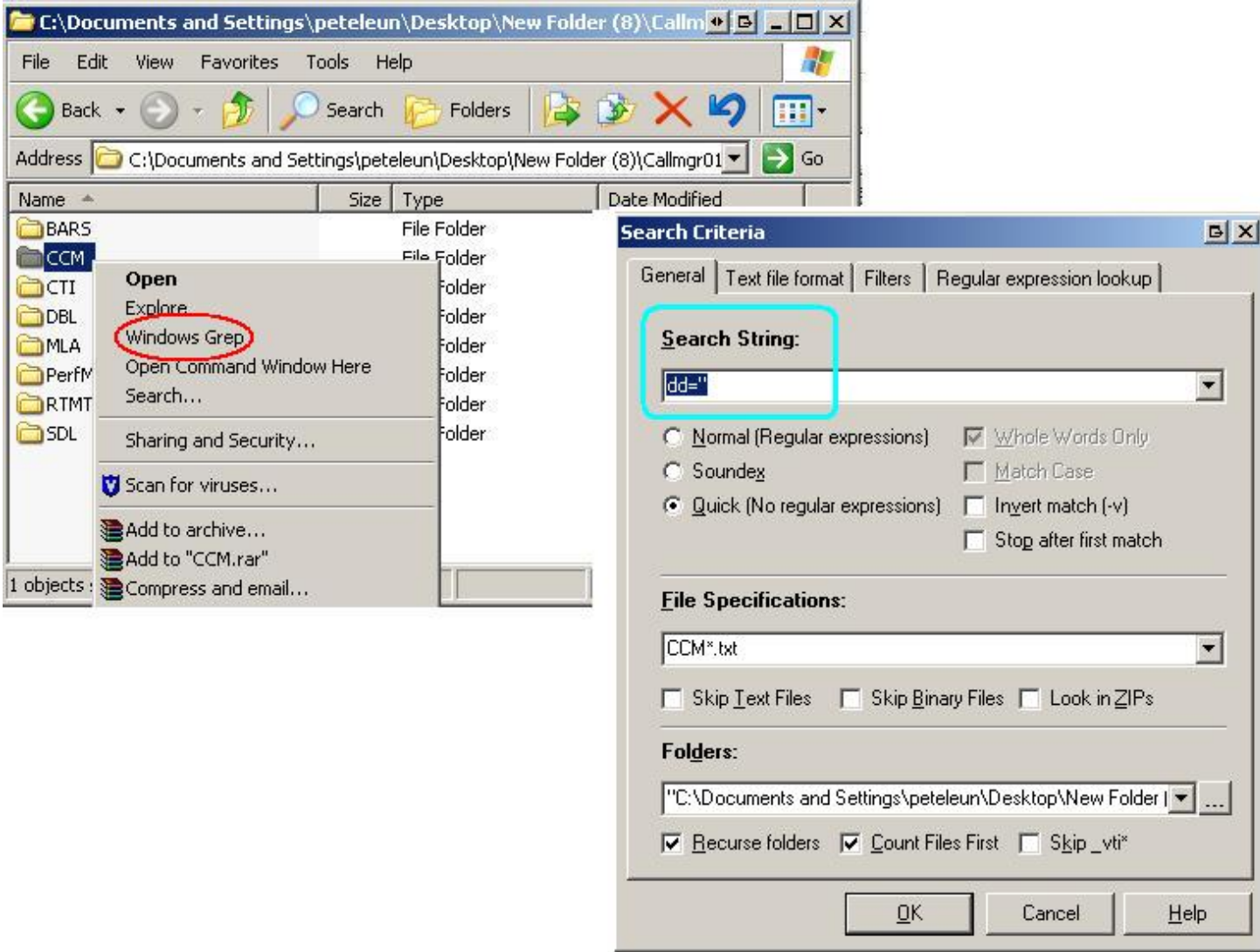
# Device Name to TCP Handle

## Correlating a Device Name to TCP Handle TCP Handle tells us the event of phone

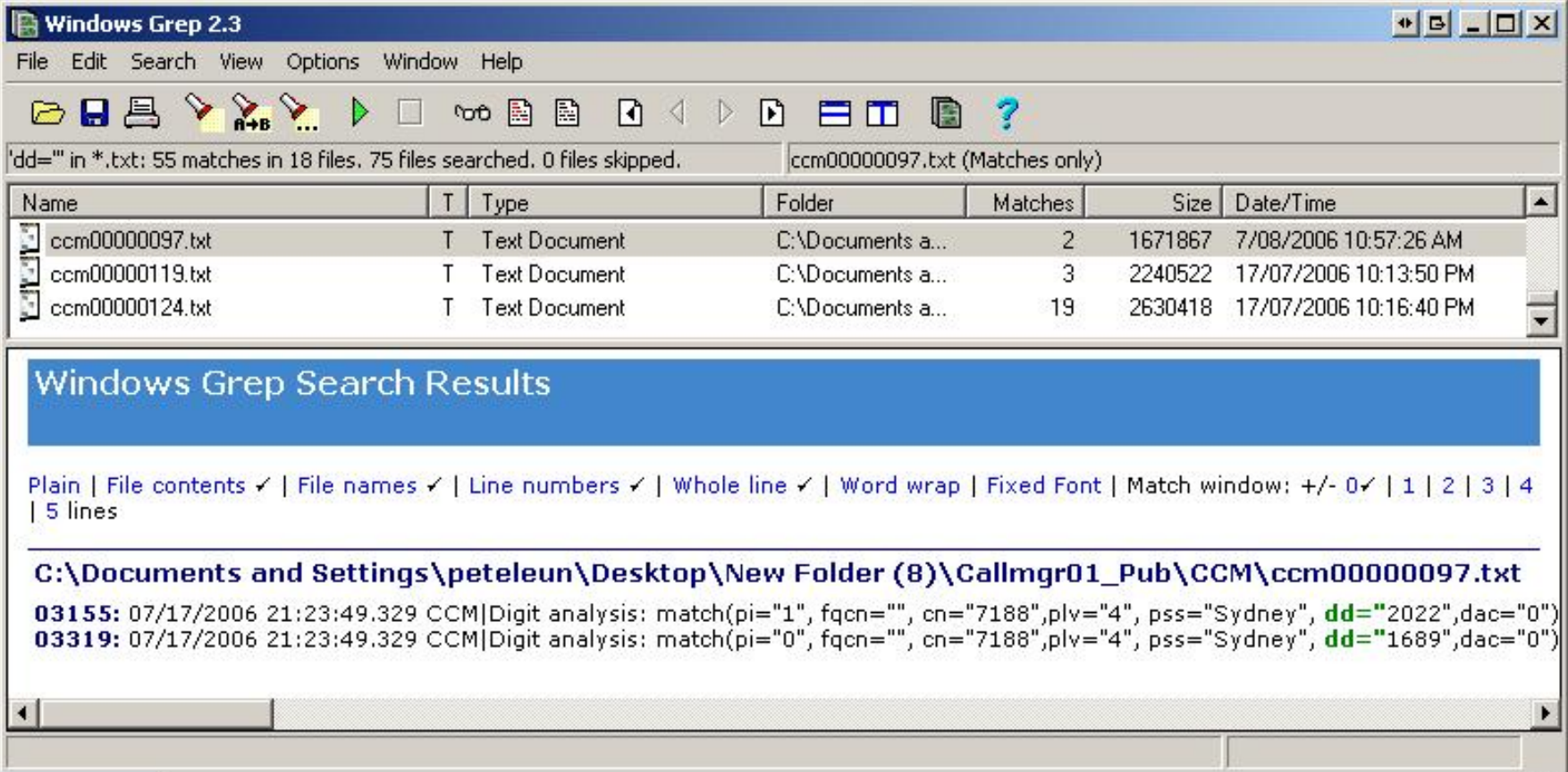
- Only way to do this reliably is by finding a KeepAlive from the phone in the trace

**\*Must select “Enable Keep Alive Trace” checkbox in CCM Trace Configuration for CCM 4.1(3) and later for Keepalives to appear in the CCM Traces**

# Searching Tool - Wingrep



# Wingrep Output



The screenshot shows the Windows Grep 2.3 application window. The title bar reads "Windows Grep 2.3". The menu bar includes "File", "Edit", "Search", "View", "Options", "Window", and "Help". The toolbar contains various icons for file operations. The status bar at the top indicates the search criteria: "dd=" in \*.txt: 55 matches in 18 files. 75 files searched. 0 files skipped." and the current file being viewed: "ccm00000097.txt (Matches only)".

Name	T	Type	Folder	Matches	Size	Date/Time
ccm00000097.txt	T	Text Document	C:\Documents a...	2	1671867	7/08/2006 10:57:26 AM
ccm00000119.txt	T	Text Document	C:\Documents a...	3	2240522	17/07/2006 10:13:50 PM
ccm00000124.txt	T	Text Document	C:\Documents a...	19	2630418	17/07/2006 10:16:40 PM

**Windows Grep Search Results**

Plain | File contents ✓ | File names ✓ | Line numbers ✓ | Whole line ✓ | Word wrap | Fixed Font | Match window: +/- 0✓ | 1 | 2 | 3 | 4 | 5 lines

**C:\Documents and Settings\peteleun\Desktop\New Folder (8)\Callmgr01\_Pub\CCM\ccm00000097.txt**

**03155:** 07/17/2006 21:23:49.329 CCM|Digit analysis: match(pi="1", fqcn="", cn="7188",plv="4", pss="Sydney", **dd="2022",dac="0"**)

**03319:** 07/17/2006 21:23:49.329 CCM|Digit analysis: match(pi="0", fqcn="", cn="7188",plv="4", pss="Sydney", **dd="1689",dac="0"**)



# Determine the TCP Handle for Simon's Phone

- 08/08/2006 20:25:27.833 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller.  
DeviceName=SEP0002FD3BAF0B, TCPPid = [2.100.137.56860],  
IPAddr=10.66.6.204, Port=0, Device Controller=[2,123,2129]

Windows Grep 2.3

File Edit Search View Options Window Help

'KeepAliveMessage' in CCM\*.txt: 7250 matches in 3 files. 3 files searched. 0 files skipped. ccm00000221.txt (Matches only)

Name	T	Type	Folder	Matches	Size	Date/
ccm00000219.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\New Folder (5)\11\CCM	4429	2351380	8/08/2006
ccm00000220.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\New Folder (5)\11\CCM	2733	2155004	8/08/2006
ccm00000221.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\New Folder (5)\11\CCM	88	195073	8/08/2006

01061: 08/08/2006 20:25:25.489 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=SEP000011110021, TCP  
01079: 08/08/2006 20:25:25.926 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=SEP000011110011, TCP  
01080: 08/08/2006 20:25:26.567 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=ANN\_10.66.88.10, TCP  
01083: 08/08/2006 20:25:27.817 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=SEP000011110018, TCP  
01084: 08/08/2006 20:25:27.833 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=SEP0002FD3BAF0B, TC  
01085: 08/08/2006 20:25:27.895 CCM|InboundStim - KeepAliveMessage - Send KeepAlive to Device Controller. DeviceName=SEP000011110024, TCP

# TCP Handle Information Gathering

- Use TCP Handle to determine activities of Simon's Phone around the time of the problem

Windows Grep 2.3

File Edit Search View Options Window Help

'0002129' in CCM\*.txt: 72 matches in 2 files. 3 files searched. 0 files skipped. ccm00000022.txt (Matches only)

Name	T	Type	Folder	Matches	Size	Date/
ccm00000020.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\callmana...	3	1839864	10/06
ccm00000022.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\callmana...	69	1599415	10/06

```
05542: 08/10/2006 15:08:05.909 CCM|StationD: (0002129) DEBUG- star_DSetCallState(8) State of cdpc(27663) is 7.|<CLID::StandAloneC
05543: 08/10/2006 15:08:05.909 CCM|StationD: (0002129) ActivateCallPlane lineInstance=1.|<CLID::StandAloneCluster><NID::10.66.88.
05545: 08/10/2006 15:08:05.909 CCM|StationD: (0002129) SetRinger ringMode=1(RingOff).|<CLID::StandAloneCluster><NID::10.66.88.1
05550: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) DEBUG- star_DSetCallPhase updateACall=16777222 from Phase=1 to callPhase
05551: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) StopTone.|<CLID::StandAloneCluster><NID::10.66.88.11><CT::1,100,142,3.
05552: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) CallState callState=5 lineInstance=1 callReference=16777222 privacy=0 prece
05554: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) DisplayPromptStatus timeOut=0 Status='€' content='Connected' line=1 CI=16
05556: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) (2,100,137,56860) CallInfo callingPartyName="" callingParty=0401252111 cgpn
05557: 08/10/2006 15:08:05.925 CCM|StationD: (0002129) DEBUG- star_DSetCallState(9) State of cdpc(27663) is 8.|<CLID::StandAloneC
05560: 08/10/2006 15:08:05.940 CCM|StationD: (0002129) StopTone.|<CLID::StandAloneCluster><NID::10.66.88.11><CT::1,100,148,3.
05561: 08/10/2006 15:08:05.940 CCM|StationD: (0002129) OpenReceiveChannel conferenceID=16777222 passThruPartyID=16777265 mil
05564: 08/10/2006 15:08:05.940 CCM|StationD: (0002129) startMediaTransmission conferenceID=16777222 passThruPartyID=16777265 r
05568: 08/10/2006 15:08:06.018 CCM|StationInit: (0002129) OpenReceiveChannelAck Status=0, IpAddr=0xcc06420a, Port=26548, PartyID
05877: 08/10/2006 15:08:27.582 CCM|StationD: (0002129) ApplicationID: 0, DataLength: 84, LineInstance: 0, CallReference: 0, tcp Length
06253: 08/10/2006 15:08:27.628 CCM|StationInit: (0002129) InboundStim - StationDeviceToUserDataResponseMessageVersion1ID: Msg S
```

# CallInfo information from CCM trace

## Inbound Call

**Extension 2303**

**Calling Party = 0401252111**

**At 15:08 p.m. on August 10, 2006**

08/10/2006 15:08:05.925 CCM|StationD: (0002129) (2,100,137,56860) CallInfo

callingParty=0401252111

calledParty=2303

originalCalledParty=2303

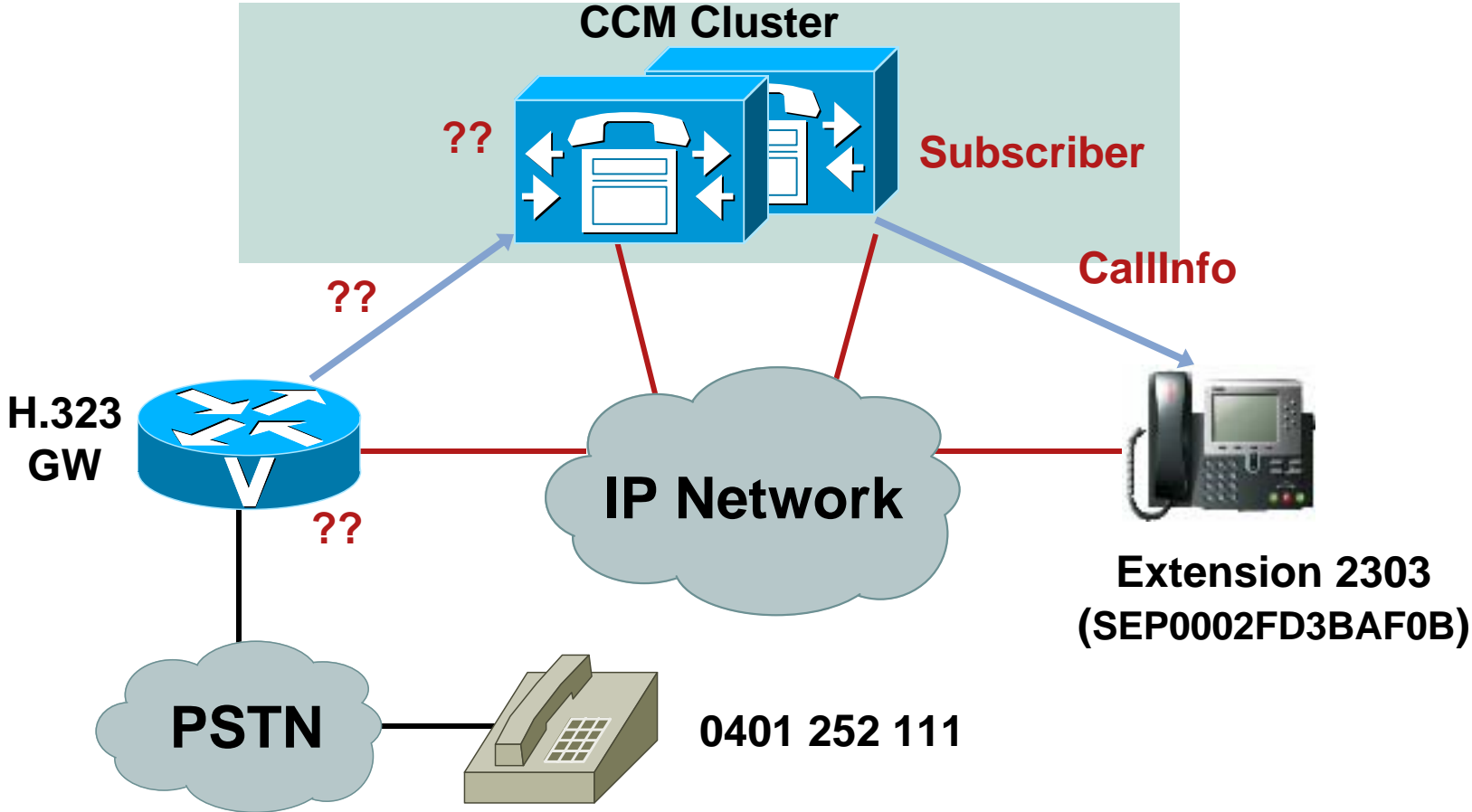
lastRedirectingParty=2303

callType=1(InBound)

lineInstance=1

**callReference=16777222**

# Call Flow Diagram



# Finding Originating Device

Where Did This Call Come from?

- Look immediately above the first messages sent to the phone in relation to this call to see if there is an inbound gateway call
- If you do not see the Digit Analysis results for this call in the trace file, the call must have originated from some other node in the cluster
- Use the SDL trace to help you find which server in the cluster (node) the call originated on

# Finding Originating Node

## Searching SDL Trace to Find Originating Node

The screenshot shows a Windows Grep 2.3 window with search results for '0002129' in CCM\*.txt files. Below the search results, a Notepad window displays an SDL trace log with the following entries:

Name	T	Type	Folder	Matches	Size	Date/Time
ccm00000020.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\callmana...	3	1839864	10/08/2...
ccm00000022.txt	T	Text Document	C:\Documents and Settings\peteleun\Desktop\callmana...	69	1599415	10/08/2...

```
05495: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) DEBUG- checkActivateRinger: retVal=4.<CLID::StandAloneCluster><NID::10.66.88.1>
05500: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) DEBUG- star_DSetCallState(0) State of cdpc(27663) is 0.<CLID::StandAloneCluster><
05501: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) CallState callState=4 lineInstance=1 callReference=16777222 privacy=0 precedenceLv
05503: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) DisplayPromptStatus timeOut=0 Status='€|0401252111' content='From 0401252111' lin
05505: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) DisplayNotify timeOutValue=10 notify='€|0401252111' content='From 0401252111' ver
05507: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) (2.100.137.56860) CallInfo callingPartyName="" callingParty=0401252111 connVoiceMai
05508: 08/10/2006 15:07:56.003 CCM|StationD: (0002129) (2.100.137.56860) CallInfo callingPartyName="" callingParty=0401252111 connVoiceMai

005802064| 06/08/10 15:07:55.753| 002| SdlSig | MGCPocTimer
005802065| 06/08/10 15:07:56.003| 002| SdlSig-I | CcSetupReq
nName= rnNamePi=0 fQOCdpn=2303 fQRN=2303 oCdpnPart= oCdpnPat=2303 oCdpn.tn=0 oCdpn.npi=C
005802066| 06/08/10 15:07:56.003| 002| Created |
005802067| 06/08/10 15:07:56.003| 002| LnkState |
005802068| 06/08/10 15:07:56.003| 002| SdlSig | Start
005802069| 06/08/10 15:07:56.003| 002| SdlSig | CcSetupReq
```

# SDL Trace File Definitions

## SDL Trace Line Example:

```
005802065| 06/08/10 15:07:56.003| 002| SdISig-I | CcSetupReq  
| idle | LineControl(2,100,50,2129) | Cdcc(1,100,23,3)
```

Field Name	Description
Line Number	Line number continuously incremented across files
Date and Time	Date and time the event occurred
Node ID	The node ID for the server where this trace is written
SDL Operation	Indicates if the signal is local to the server (SdISig), inbound from another node in the cluster (SdISig-I), or out to another node in the cluster(SdISig-O)
SDL Signal Name	The signal that is being sent from source process to destination process
Destination Process State	Current state machine state of the destination process
Destination Process	The name and process ID of the destination process
Source Process	The name and process ID of the source process

# SDL Trace File Definitions

## What Does Cdcc(1,100,23,3) Mean?

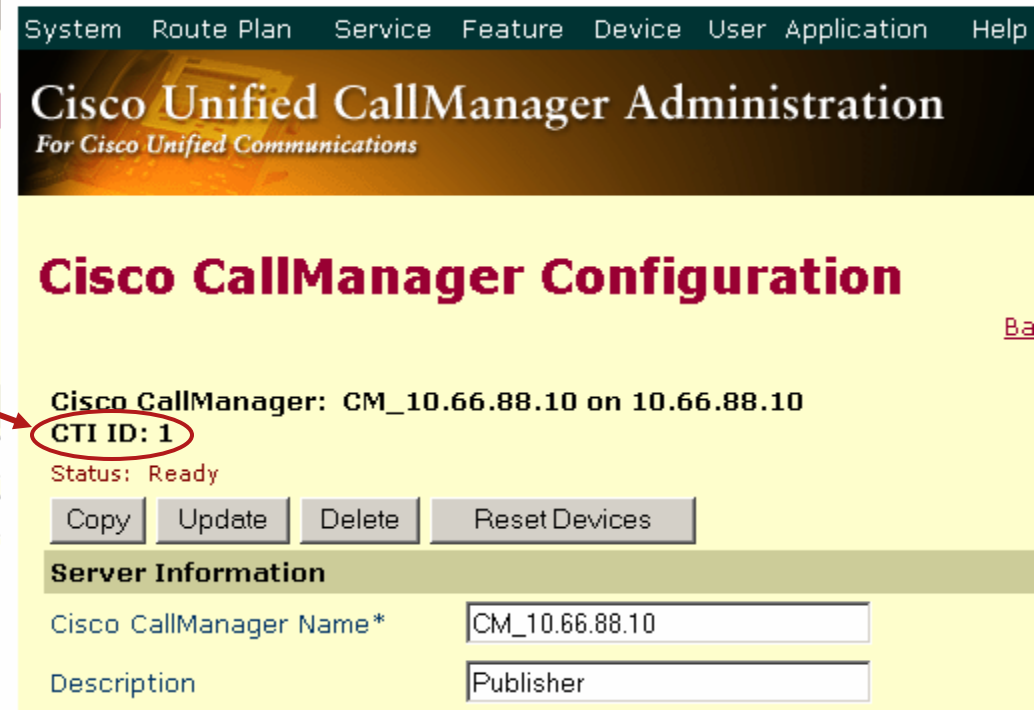
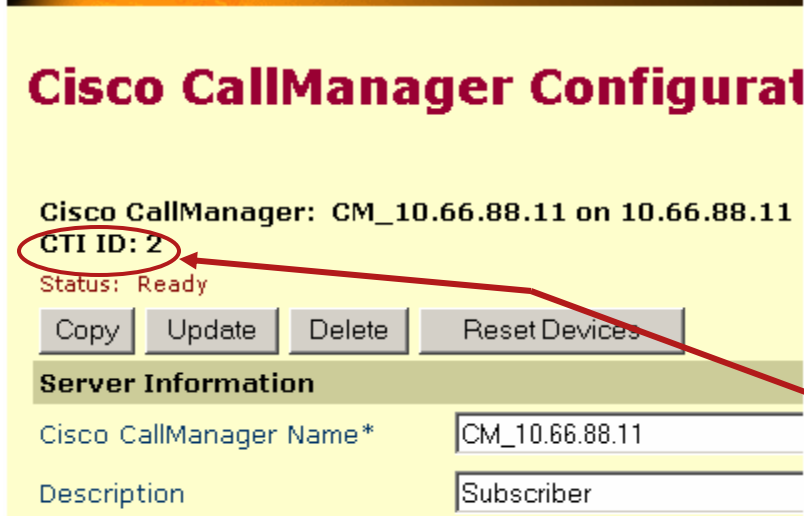
Cdcc(Node ID, Application ID, PID, PInstance)

Field Name	Description
Node ID	Node in the cluster where this process exists
Application ID	100 = Cisco CallManager, 200 = CTIManager
Process ID	In this case 23 means Cdcc; process IDs are assigned at runtime and will not be the same from one Cisco CallManager restart to another
Process Instance	The instance ID of this process; in this case this is the 3rd Cdcc process that has been created



# Finding SDL Node ID

## Node ID Is Found Under System > Cisco CallManager



# Finding Originating Node

## Going Back to the SDL Trace Line

```
005802065| 06/08/10 15:07:56.003| 002| SdISig-I | CcSetupReq  
| idle | LineControl(2,100,50,2129) | Cdcc(1,100,23,18)
```

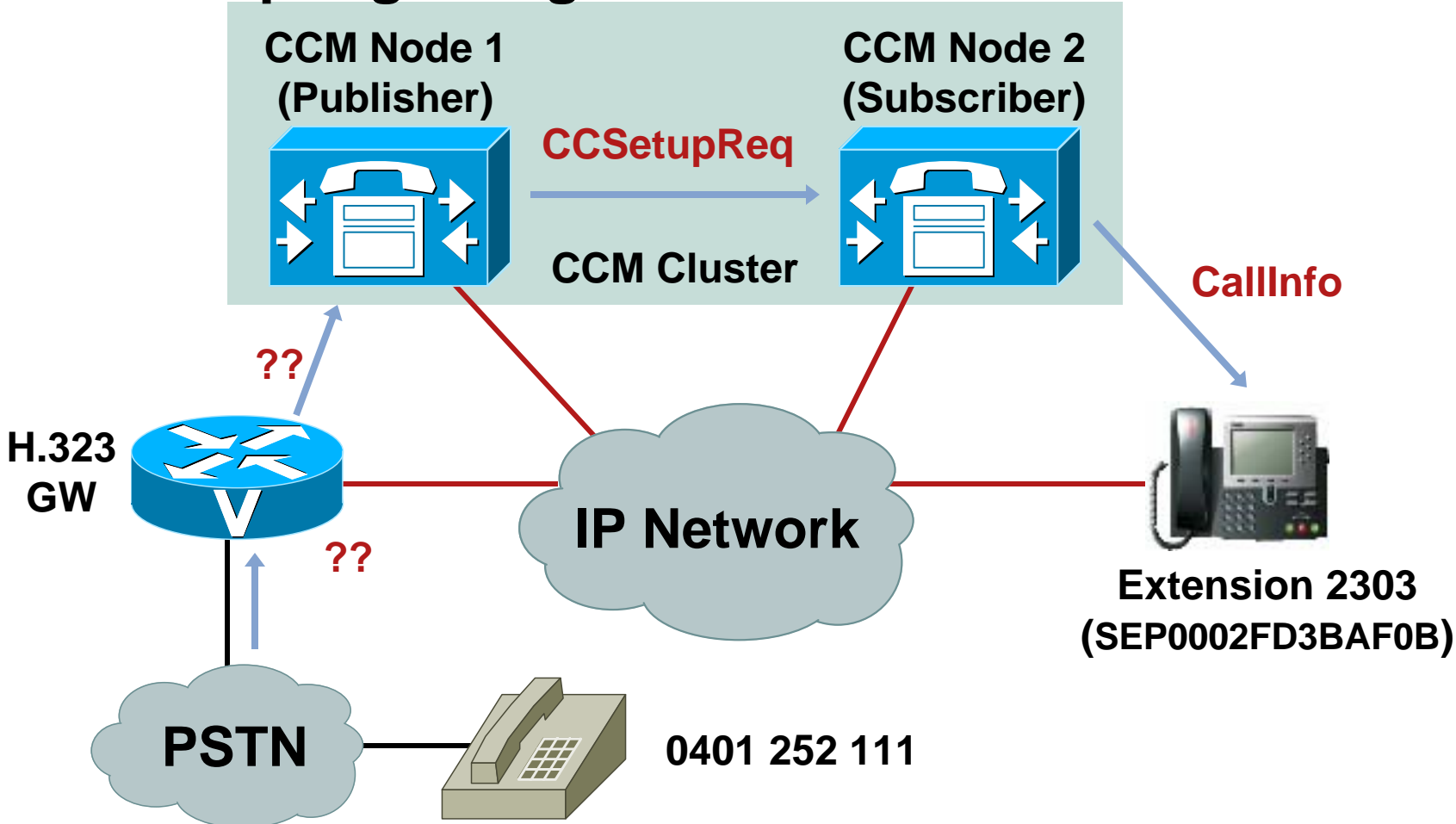
- This means the call originated on Node 1
- Look in the SDL trace on Node 1 to find the matching trace line

```
000004494| 06/08/10 15:07:56.002| 001| SdISig-O | CcSetupReq  
| NotApplicable_RemoteSignal | LineControl(2,100,50,2129) | Cdcc(1,100,23,3)
```

- So now look in CCM trace at 06/08/10 15:07:56.003 on Node 1 (Publisher)

# Call Setup

## Call Setup Signaling



# Found Digit Analysis Results

**CCM Trace at 08/10/2006 15:07:56.002**

08/10/2006 15:07:56.002 CCM|Digit analysis: analysis results

|PretransformCallingPartyNumber=**0401252111**

|CallingPartyNumber=0401252111

|DialingPartition=

|DialingPattern=**2303**

|FullyQualifiedCalledPartyNumber=2303

..

..

..

|VoiceMailPilotNumber=

|AlertingName=

|RouteBlockFlag=RouteThisPattern

# Found Originating SETUP

## Look Just Before the Digit Analysis Match and You See:

08/10/2006 15:07:56.002 CCM|In Message -- H25SetupMsg -- Protocol= H25Protocol  
08/10/2006 15:07:56.002 CCM|le - H25BearerCapabilityle -- IEData= 04 03 80 90 A3  
08/10/2006 15:07:56.002 CCM|le - H25CallingPartyle -- IEData= 6C 0B 80 30 34 30 31 32 35 32 31 31 31  
08/10/2006 15:07:56.002 CCM|le - Q931CalledPartyle -- IEData= 70 05 80 32 33 30 33

The screenshot shows a network analysis tool interface with two main sections: 'Messages' and 'Messages Translation'.

**Messages Table:**

R	Timestamp	Device IP	Direction	Protocol	Message	(CallRef)	Cha
	08/10/2006 15:07:56.002	10.66.90.3	Receive	H.225	SETUP	0x0009	
	08/10/2006 15:07:56.002	10.66.90.3	Send	H.225	CALL_PROC	0x8009	
	08/10/2006 15:07:56.017	10.66.90.3	Send	H.225	ALERTING	0x8009	
	08/10/2006 15:07:56.017	10.66.90.3	Send	H.225	NOTIFY	0x8009	
	08/10/2006 15:08:05.924	10.66.90.3	Send	H.225	CONNECT	0x8009	

**Messages Translation:**

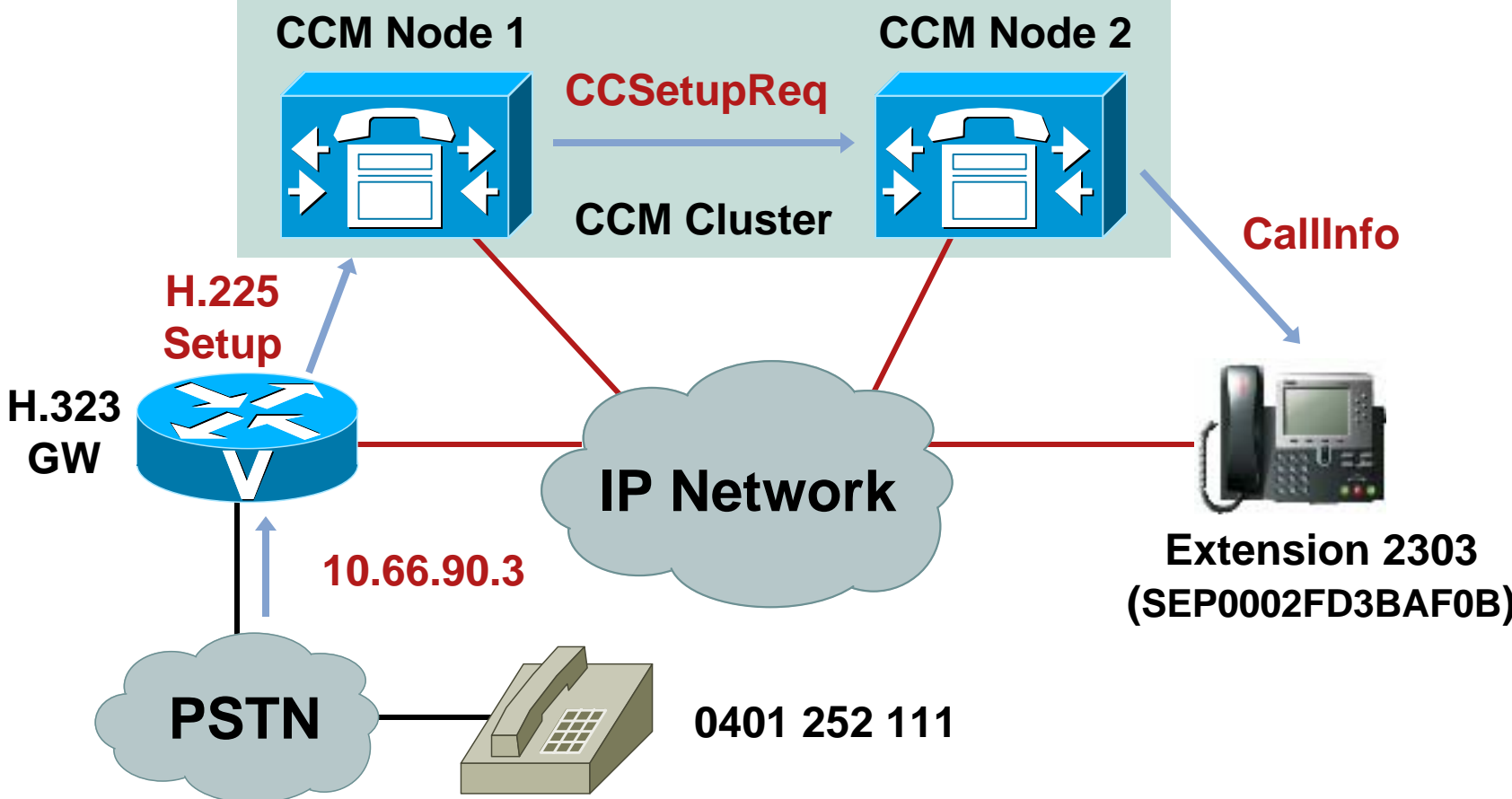
Raw  Simple  Detailed

```
SETUP, pd = 8, callref = 0x0009
Bearer Capability i = 0x0800900A3, ITU-T standard, Speech, Circuit mode, 64k, A-law
Calling Party Number i = '0401252111' - Plan: Unknown, Type: Unknown
Called Party Number i = '2303' - Plan: Unknown, Type: Unknown
User-User i = 0x502008060809104A0402800B500012040103c51000BE0510520c20270640110DB080A00160
```

File: ccm00000080.txt

# Call Setup

## Call Setup Signaling



# Call Disconnected at Gateway

## Filter the Call by Call Reference to See All Messages About This Call

R	Timestamp	Device IP	Direction	Protocol	Message	(CallRef)	Chann
	08/10/2006 15:07:56.002	10.66.90.3	Receive	H.225	SETUP	0x0009	
	08/10/2006 15:07:56.002	10.66.90.3	Send	H.225	CALL_PROC	0x8009	
	08/10/2006 15:07:56.017	10.66.90.3	Send	H.225	ALERTING	0x8009	
	08/10/2006 15:07:56.017	10.66.90.3	Send	H.225	NOTIFY	0x8009	
	08/10/2006 15:08:05.924	10.66.90.3	Send	H.225	CONNECT	0x8009	
	08/10/2006 15:08:05.924	10.66.90.3	Send	H.225	NOTIFY	0x8009	
	08/10/2006 15:09:21.144	10.66.90.3	Send	H.225	RELEASE_COMP	0x8009	
	08/10/2006 15:09:27.426	10.66.90.3	Receive	H.225	RELEASE_COMP	0x0009	

- Call was originated at 15:07:56.002 and connected at 15:08:05.924
- Call was disconnected at 15:09:21.144
- Click on RELEASE\_COMP message for details

```
RELEASE_COMP, pd = 8, callref = 0x8009
Cause i = 0x0800A9 - Temporary failure
User-User i = 0x502508060809104A02101100BE0510520c20270640110DB08001C0AF0650790220B902FA0
```

- Now we know Cisco CallManager sent a Disconnect with a cause code of Temporary Failure at 15:09:21.144—but why?

# Call Dropped on IP Phone

## Go Back to the IP Phone to See What Happened from the User's Perspective

R	Timestamp	Device IP	Direction	Protocol	Message	(CallRef)	Ch
	08/10/2006 15:08:05.940	10.66.88.11		SCCP	startMediaTransmission	16777222	
	08/10/2006 15:08:06.018	10.66.88.11	Receive	SCCP	OpenReceiveChannelAck	16777222	
	08/10/2006 15:08:27.582	10.66.88.11		SCCP	ApplicationID:	16777222	
	08/10/2006 15:08:27.628	10.66.88.11		SCCP	InboundStim	16777222	
	08/10/2006 15:08:27.628	10.66.88.11	Receive	SCCP	DeviceToUserDataRespon...	16777222	
	08/10/2006 15:08:37.629	10.66.88.11		SCCP	DEBUG-	16777222	
	08/10/2006 15:08:37.629	10.66.88.11	Send	SCCP	DisplayPromptStatus	16777222	

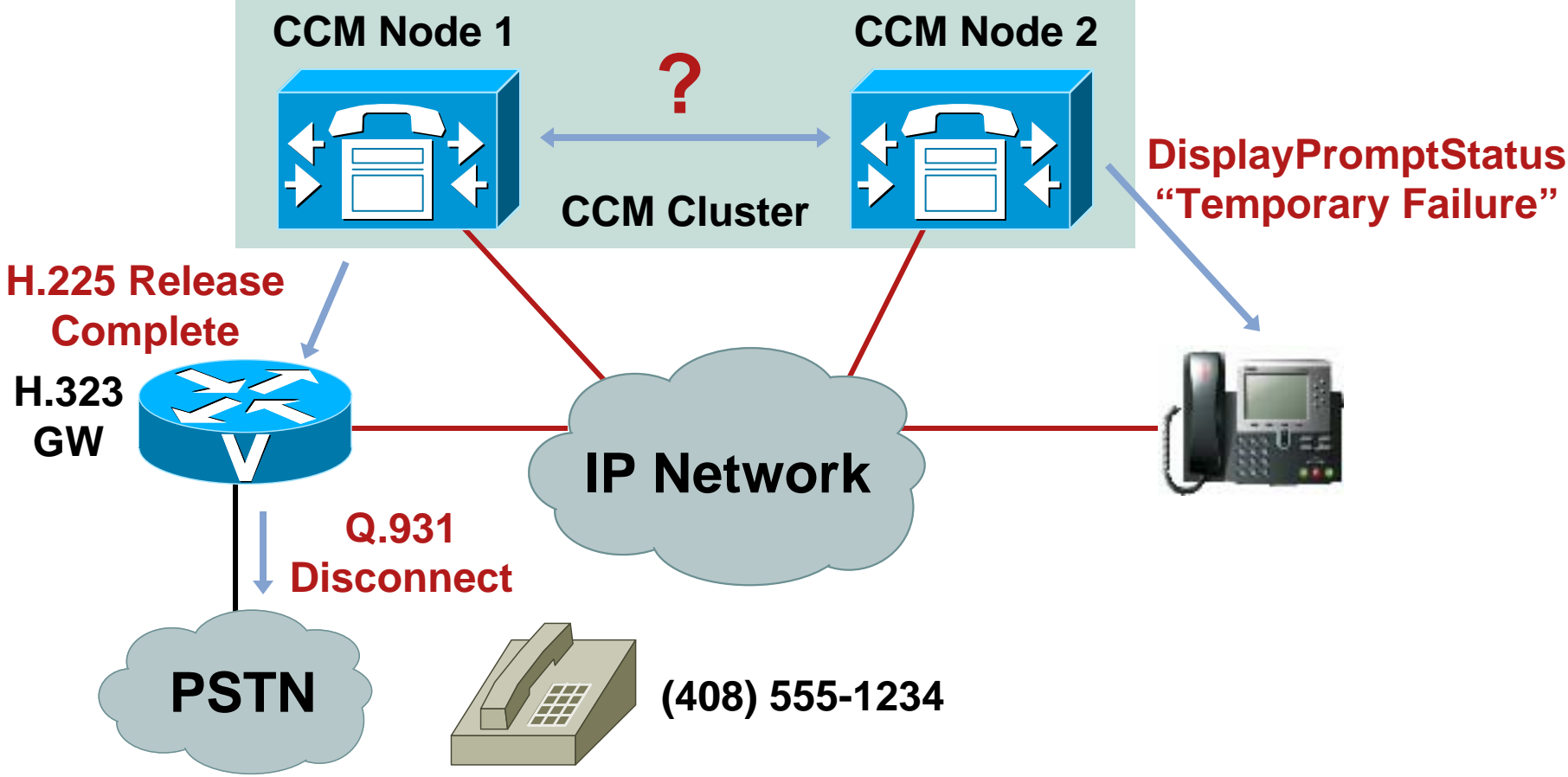
- Media streams for the call established at 15:08:05.940
- Cisco CallManager sends a DisplayPromptStatus message at 15:08:37.629; click on DisplayPromptStatus to see what the message sent to the phone was

08/10/2006 15:08:37.629 CCM|StationD: (0002129) DisplayPromptStatus  
timeOut=0 Status='€#' content='Temporary failure' line=1 Cl=16777222



# Call Disconnected

## Call Being Disconnected



## SDL Link OOS

### What Happened Between Node 1 and Node 2?

- Look at the CCM trace on Node 2 right before Cisco CallManager tells the phone about the failure at 15:08:37.629

08/10/2006 15:08:37.629 CCM|SdlinkOOS nodeId = 1, applId = 100

08/10/2006 15:08:37.629 CCM|SDLLinkOOS - SDL link to remote application out of service.

Local node ID:2 Local Application ID.:100

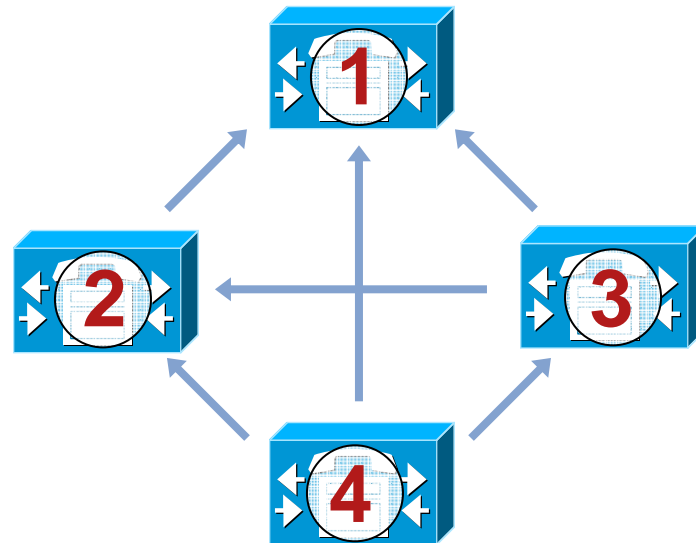
Remote IP address of remote application:10.66.88.10

RemoteNodeID:1 Remote application ID.:100

# SDL Links

## What Is an SDL Link?

- Fully meshed TCP connections between all nodes in a Cisco CallManager cluster
- Each server establishes a TCP connection to other nodes with a lower node ID than itself on port 8002



# SDL Link OOS

## Why Would an SDL Link Go Out of Service?

- IP Connectivity Issues
  - Duplex Mismatch between CCM NIC and switch
  - Router or Switch failure between CCM nodes
  - Cabling Issues
  - Network Congestion
- Cisco CallManager Restart
- Cisco CallManager unable to keep up with signals being sent across SDL Link
  - Overloaded Cisco CallManager node
  - High CPU due to other process on the system
  - High Disk I/O
  - Low Memory (causing memory to swap to/from disk)

# CMProcMon

## Check for Resource Constraints on Node 1

- CMProcMon runs every two seconds which acts like an internal KeepAlive mechanism to ensure the SDL Signal Router is still processing signals
- Before the SDL Link OOS, you can see things are working properly:

```
15:06:43.672 CCM|CMProcMon - -----Entered Router Verification
15:06:45.672 CCM|CMProcMon - -----Entered Router Verification
15:06:47.672 CCM|CMProcMon - -----Entered Router Verification
15:06:49.672 CCM|CMProcMon - -----Entered Router Verification
15:06:51.672 CCM|CMProcMon - -----Entered Router Verification
```

# Dropped Call

- After 15:08:15, big gap appear:

```
15:08:09.783 CCM|CMProcMon - -----Entered Router Verification  
15:08:11.783 CCM|CMProcMon - -----Entered Router Verification  
15:08:13.783 CCM|CMProcMon - -----Entered Router Verification  
15:08:15.799 CCM|CMProcMon - -----Entered Router Verification  
15:09:06.175 CCM|CMProcMon - -----Entered Router Verification  
15:09:13.082 CCM|CMProcMon - -----Entered Router Verification
```

**Look for problems between 15:08:15 and 15:09:06**

**So most likely reason for SDL link OOS is a resource constraint on the Node 1 - lack of CPU, memory, or disk I/O**

## Dropped Call: Summary

**We Know the Call Was Dropped Because an SDL Link Went Out of Service due to a Resource Issue on Cisco CallManager; What Can We Do About It?**

- Monitor resources on Cisco CallManager using Performance Monitor
- Check for any applications or services installed that are not certified for use on Cisco CallManager
- Check for any administrative activity on the server at the time of the problem

# Finding Resource Problem

- Cisco CallManager 4.x and later automatically keep logs of CPU and memory statistics
- To view reports, go to **Cisco CallManager Serviceability > Tools > Serviceability Reports**

**Serviceability Reports Archive**

RTMT Reports Status : Ready






Apr 2005

To view reports, click on the link corresponding to the Day for which the reports have been generated.

Apr										
01	02	03	04	05	06	07	08	09	10	11
12	13	14	15	16	17	<b>18</b>				

Click on the files to open them.

Files for Apr 18 2005

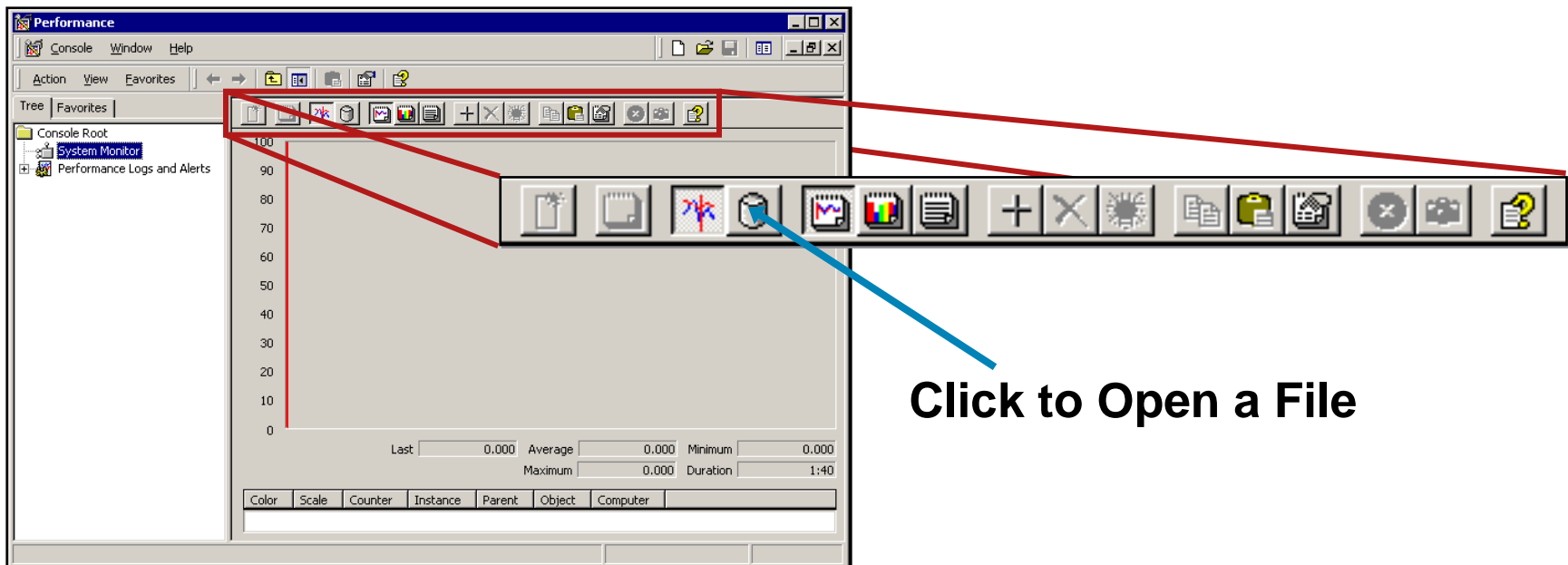
-  [Alert Report \(AlertRep\\_04\\_18\\_2005.pdf\)](#)
-  [Call Activities Report \(CallActivitiesRep\\_04\\_18\\_2005.pdf\)](#)
-  [Device Statistics Report \(DeviceRep\\_04\\_18\\_2005.pdf\)](#)
-  [Server Statistics Report \(ServerRep\\_04\\_18\\_2005.pdf\)](#)
-  [Service Statistics Report \(ServiceRep\\_04\\_18\\_2005.pdf\)](#)

Mar 2005






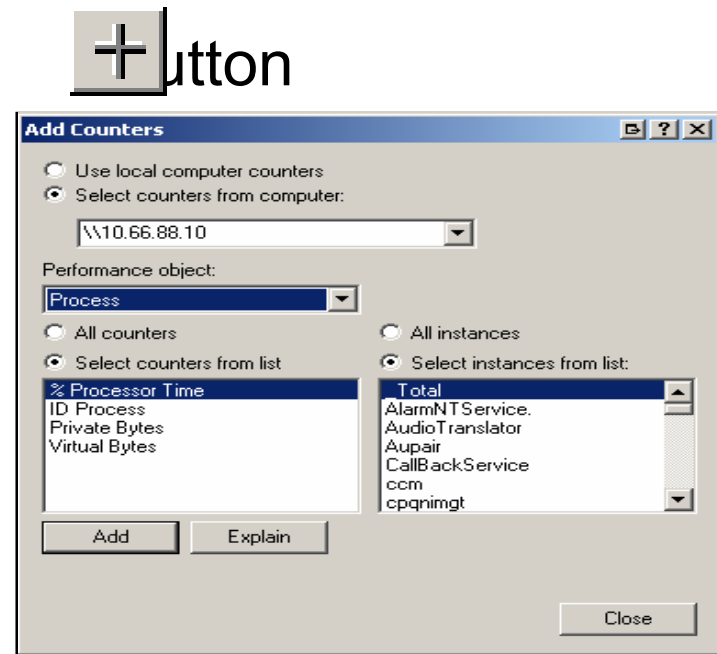
# Performance Statistics

- All data used to generate reports is stored in  
C:\Program Files\Common Files\Cisco\Logs\RTMTLoggeron  
the Publisher
- Data is stored in CSV format
- Can be read by Excel or Microsoft Performance

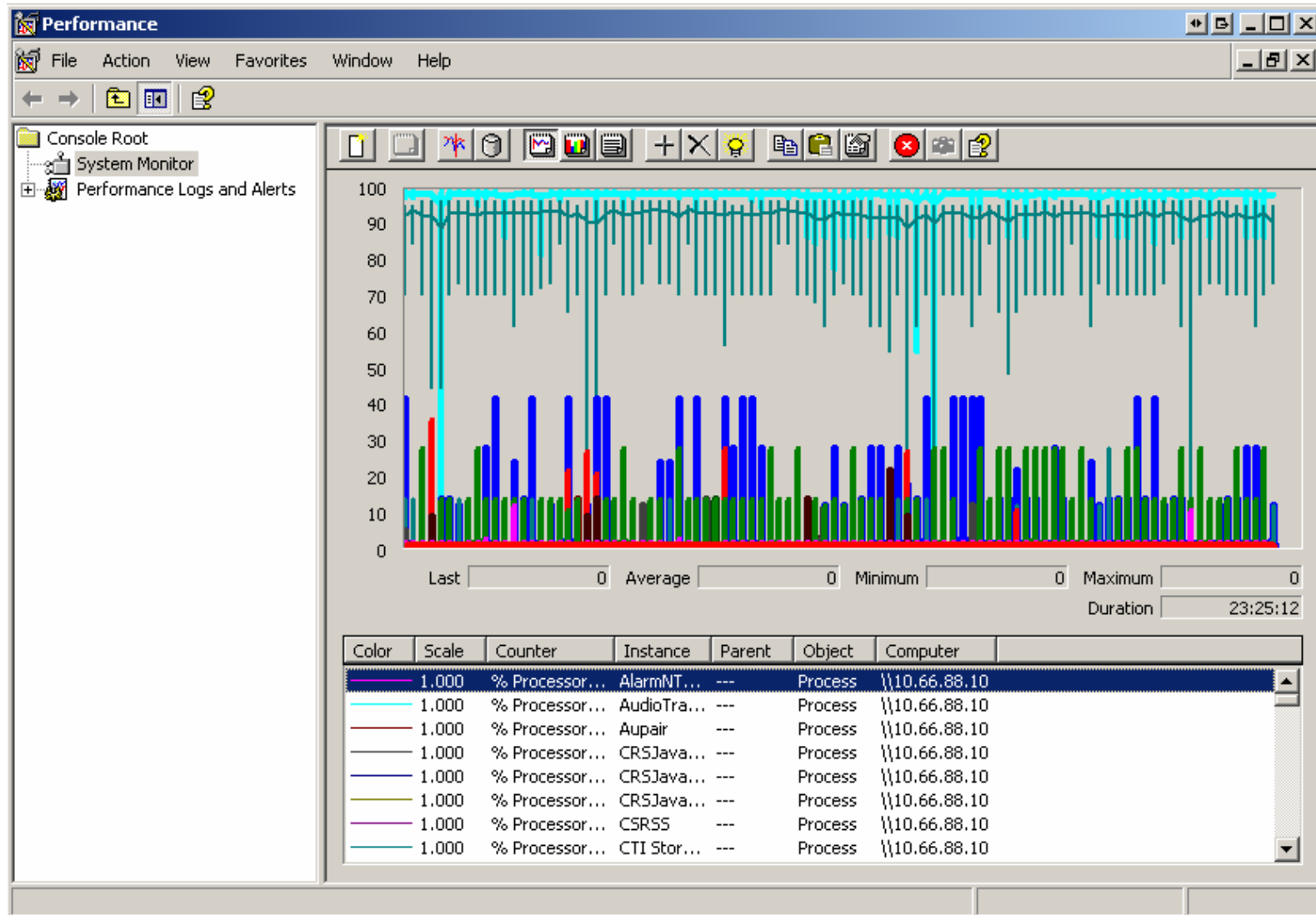


# Per Process Statistics


- Per-process CPU and Memory statistics are stored in the files named:  
**PerfMonLog\_10.66.88.10\_08\_10\_2006\_00\_00.csv**
- Each file has the Server IP Address and Date in the name
- Once the file is open, click the  button
- Select 'All Instances' for the '% Processor Time' counter
- Click the  button
- Click the  button

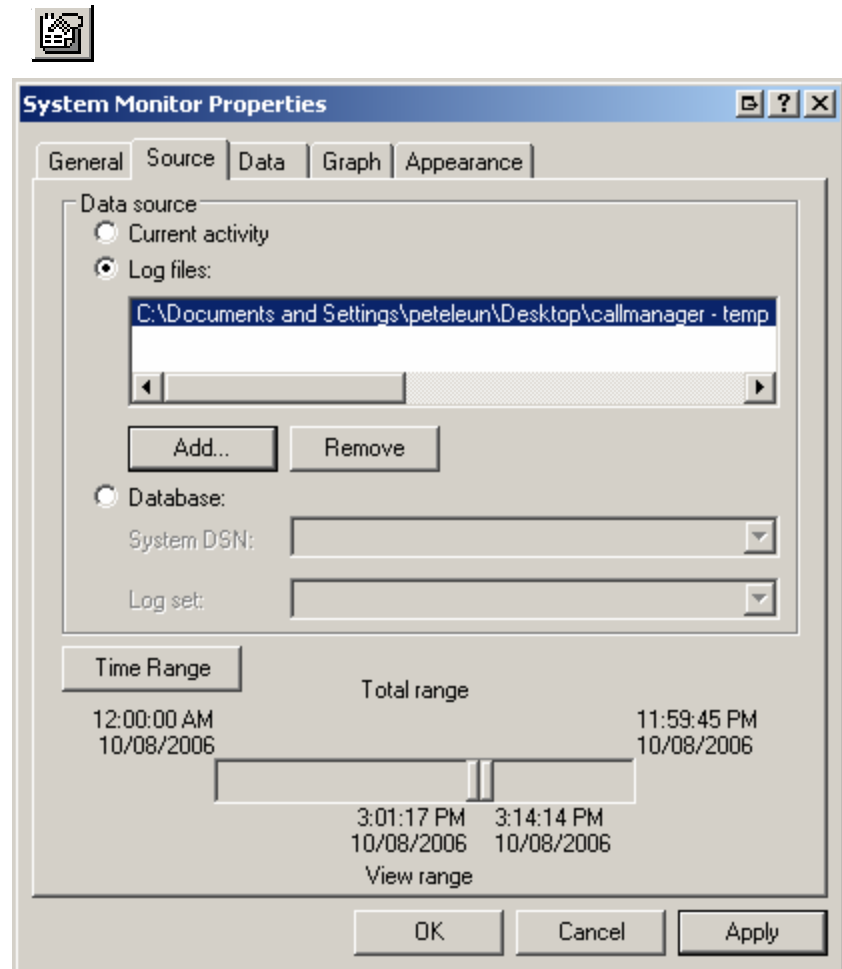


# Per Process Statistics



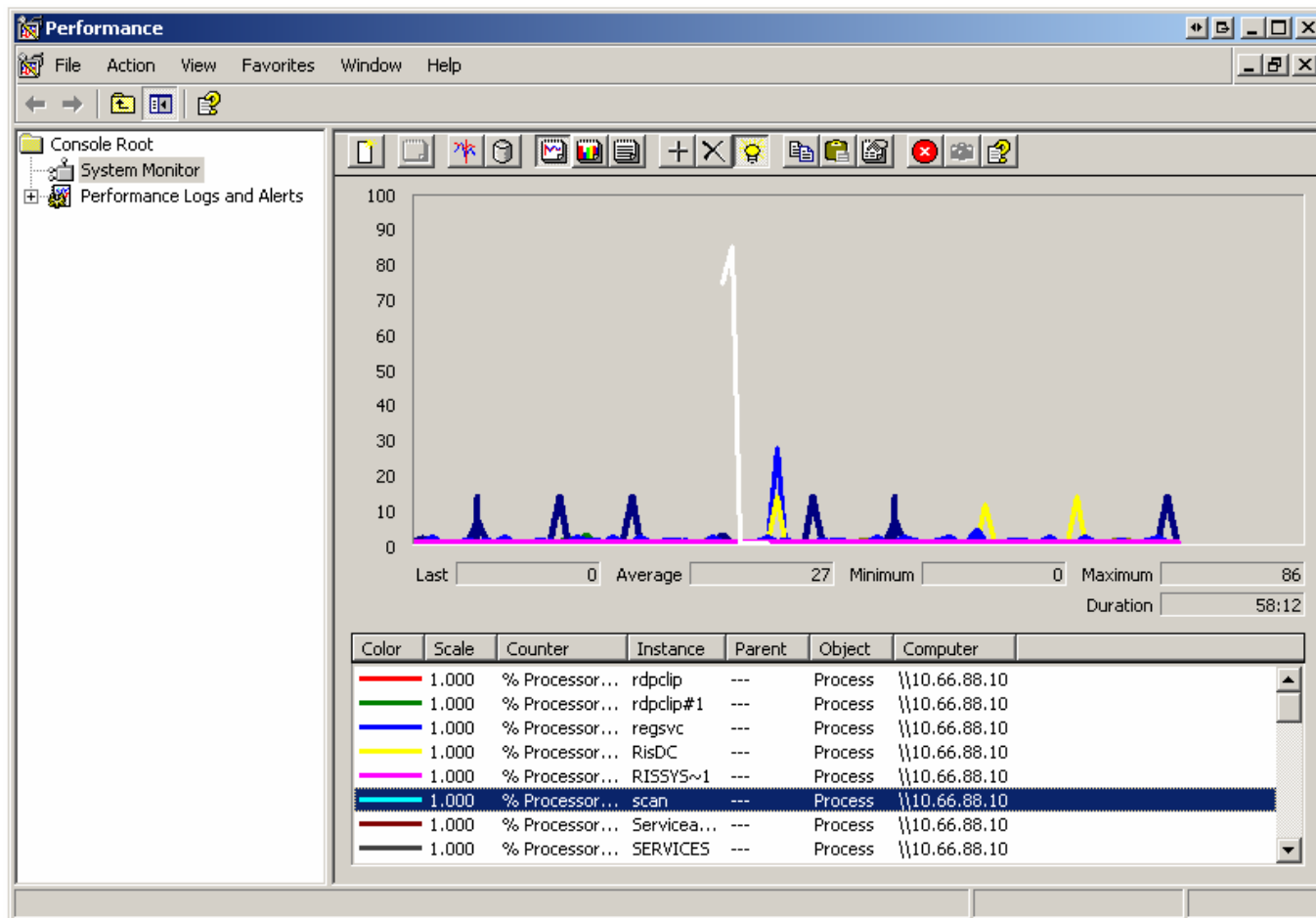
# Per Process Statistics

- Click the “Properties” Button (  )
- Select the “Source” Tab
- Adjust the “Time range” slider at the bottom to narrow down the range to the time you had a problem
- Click “OK”



# Per Process Statistics

Click the “Highlight” Button, Then Scroll Through the List Until the Spike on the Graph Is Highlighted



# Conclusion

- Using SDL and SDI traces determine the actual flow of the call
- Identify why component in the flow was causing the disconnect
- Using Logs on the call manager to determine the root cause of the CPU problem



# Agenda

- Introduction
- Company Overview
- Case Study 1: Dropped Call
- **Case Study 2: Intermittent voice quality issue**

## Problem 2 – Voice quality

“Hello Peter, need your help again! This time the users in Melbourne are reporting poor voice quality intermittently. It seems very random. “

“What should I do??”



# Problem Description

- What type of calls are experiencing the problem? -  
phone to phone? (same site? Different site?)
  - Gateway to phones?
  - When is it happening?
  - Can the problem be reproduced?
  - How often is it happening?
  - Who is hearing the bad audio? (One-way? Both ways?)

# Problem Update

- Only happen for calls between Brisbane and Melbourne.
- Sometimes audio is bad for the whole call and sometimes part of the call.
- Hanging up and reconnecting the call doesn't seem to fix the problem.
- User normally tries again after awhile and the problem is gone

# Common Voice Quality issues

- Voice quality issue is mostly caused by network related issues.
- But I don't have any user reports of issues with data traffic??
  - Voice traffic more sensitive to network problems
  - Voice path vs data path

# What to collect?

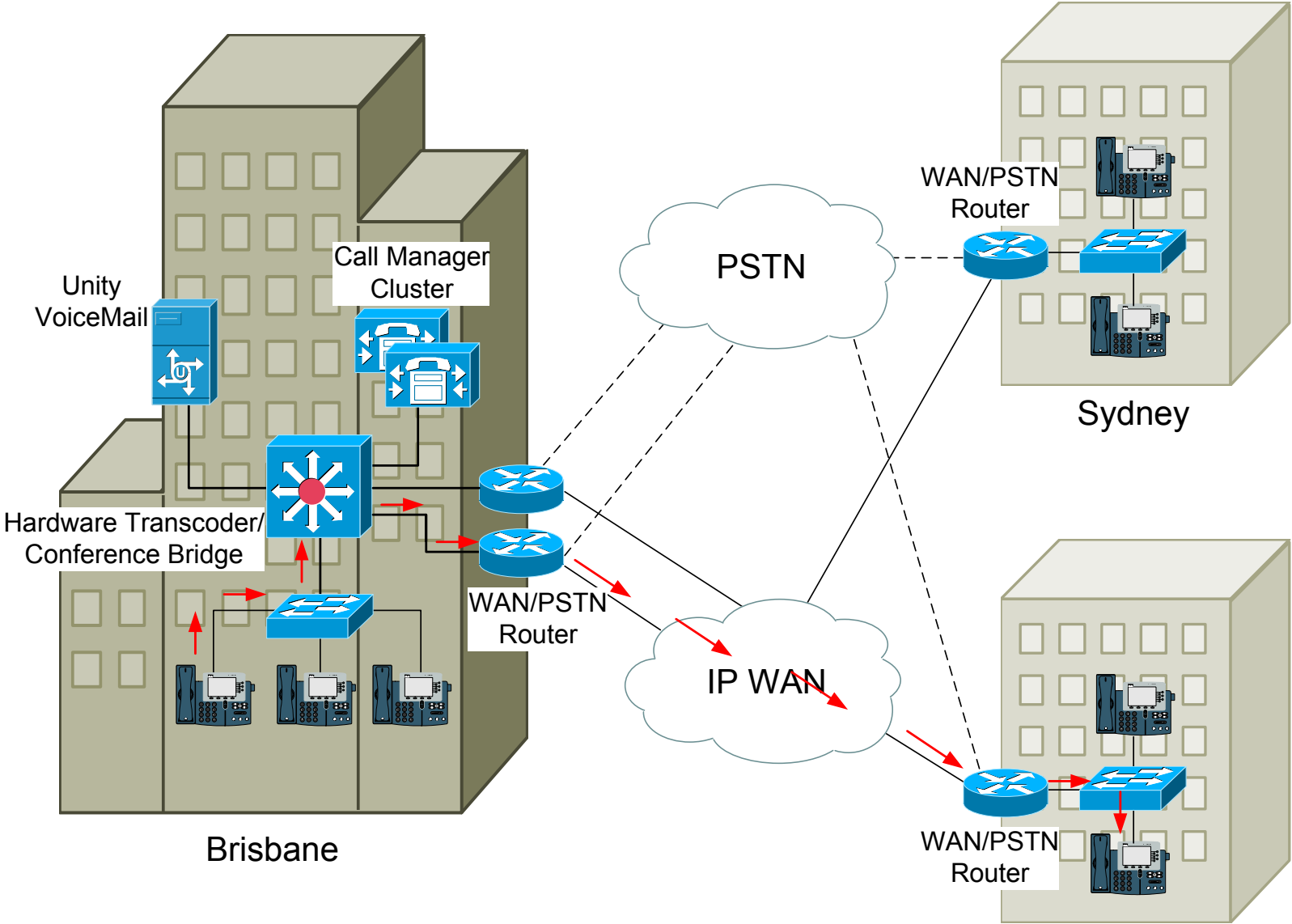
- Call manager traces
- Sniffer traces
- Ensure network path is clean (clear counter on all devices and monitor)
- Confirm phone setting is correct (incorrect settings, e.g location)
- Pattern to the problem (time of day? Location?)

# Ring Ring

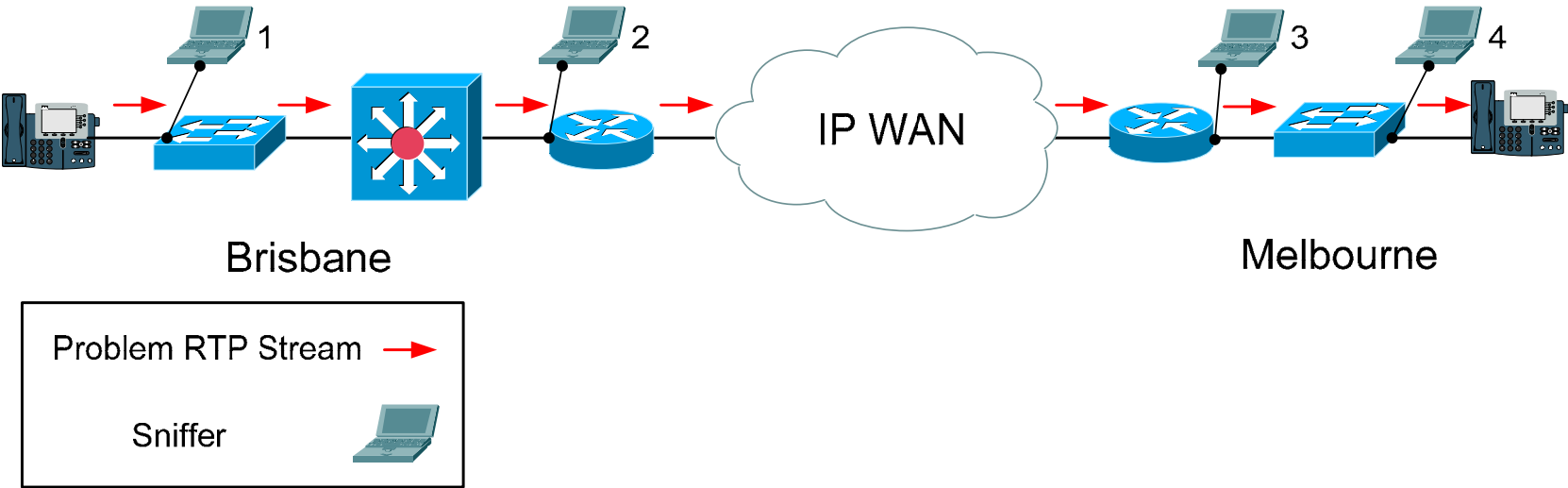
“Hi Pete, a user has just reported the problem. As previously reported, the user is Melbourne is experiencing the poor audio.”



# Call Flow Diagram



# Simplified Call Flow Diagram



# Tools Break - Extracting Audio Stream

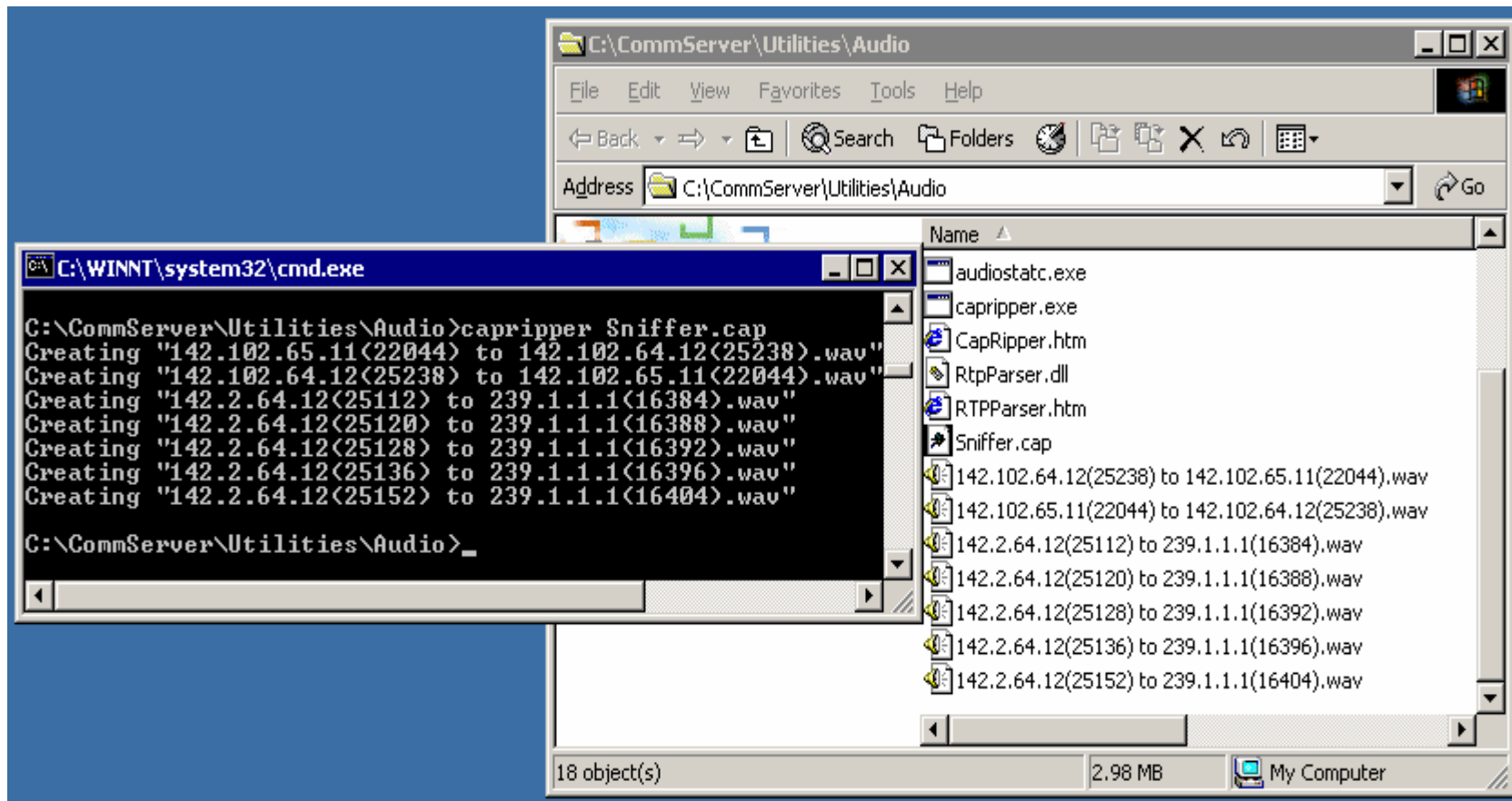
- Capripper
- Ethereal
- RTPPlay





# Capripper

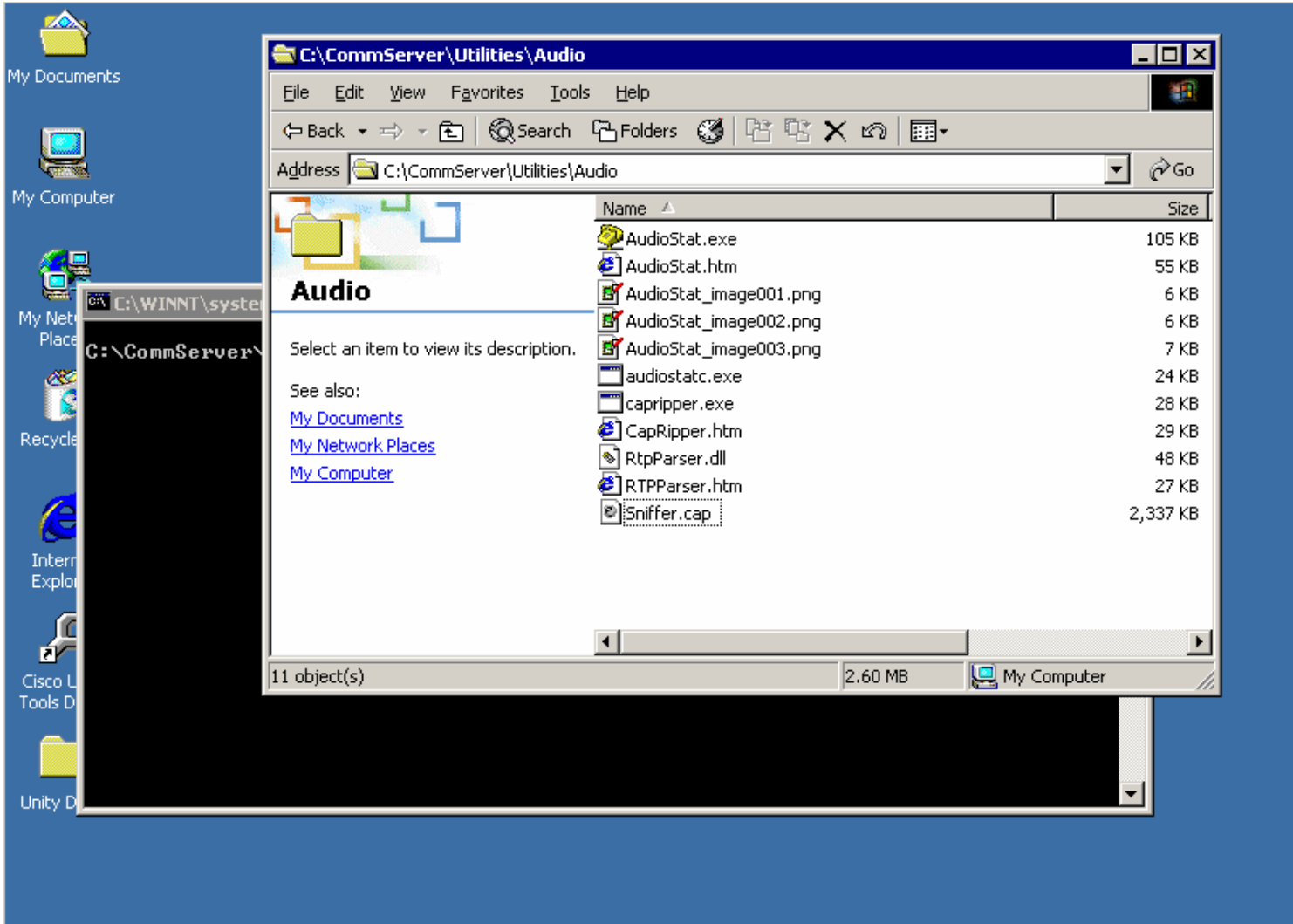
- C:\CommServer\Utilities\Audio
- Installed by default on Unity server



# Capripper

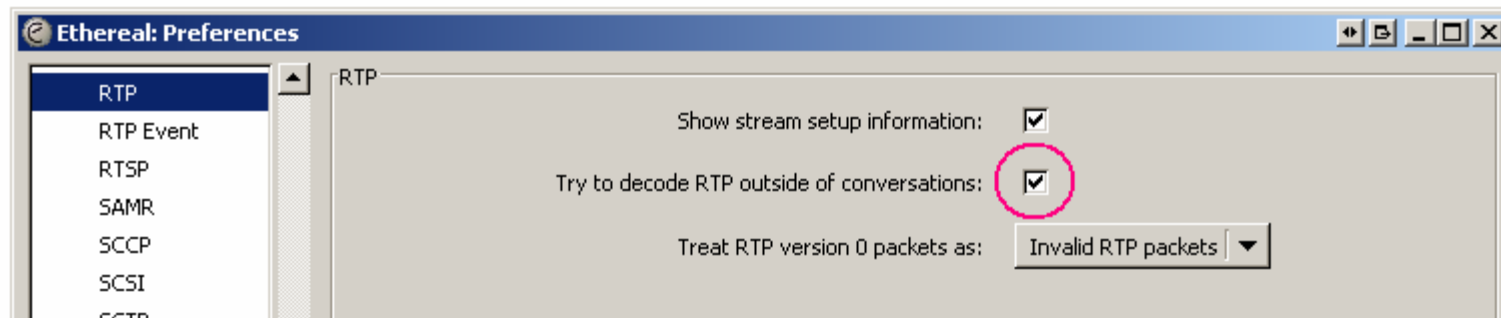
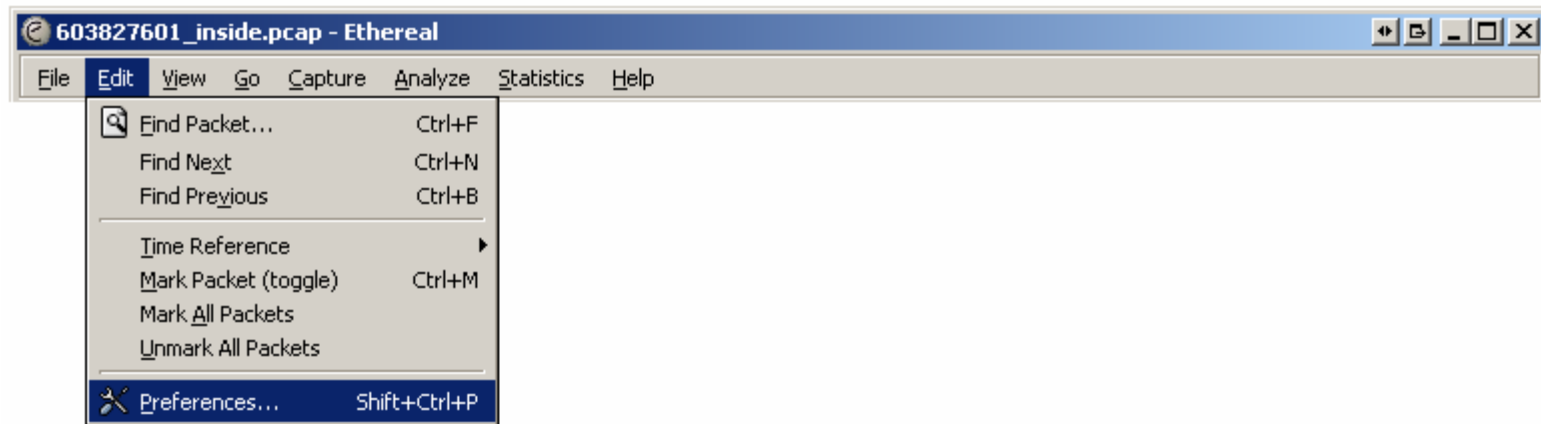
- C:\CommServer\Utilities\Audio>capripper
- Usage: capripper [-d numBytes] [-o offset] [-s] [filename]
- Options:
  - -d number of bytes to dump
  - -o offset in bytes to start extracting data (NetMon only)
  - -s display summary information about RTP packets

# Capripper Demo



# Ethereal - Sniffer Trace Analysis

- Check “Try To decode RTP outside of conversations”



# Sniffer - Ethereal

- Statistics -> RTP -> Stream Analysis...

Ethereal: RTP Stream Analysis

Forward Direction | Reversed Direction

Analysing stream from 10.100.81.254 port 19300 to 10.100.86.10 port 20644 SSRC = 219632126

Packet #	Sequence	Delta (ms)	Jitter (ms)	BW (kbps)	Marker	Status
3	54737	0.00	0.00	1.60		[ Ok ]
15	54738	19.92	0.00	3.20		[ Ok ]
28	54739	20.00	0.00	4.80		[ Ok ]
40	54740	20.10	0.01	6.40		[ Ok ]
51	54741	19.92	0.02	8.00		[ Ok ]
63	54742	20.02	0.02	9.60		[ Ok ]
76	54743	20.04	0.02	11.20		[ Ok ]
89	54744	20.03	0.02	12.80		[ Ok ]
102	54745	19.97	0.02	14.40		[ Ok ]

Max delta = 0.029947 sec at packet no. 2583  
Total RTP packets = 10850 (expected 10850) Lost RTP packets = 0 (0.00%) Sequence errors = 0

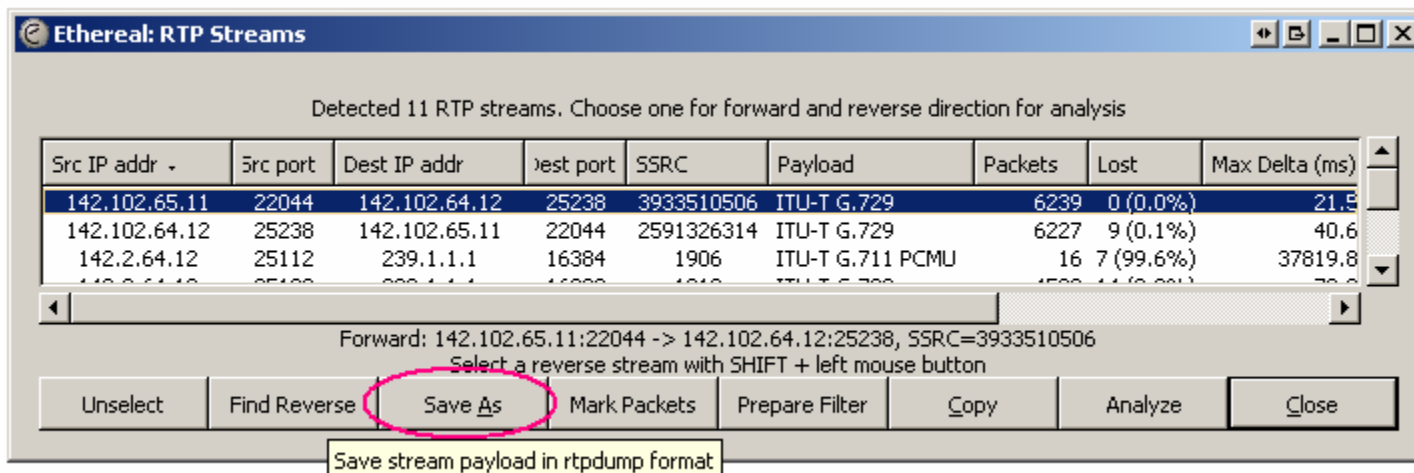
Save payload... | Save as CSV... | Refresh | Jump to | Graph | Next non-Ok | Close

# RTPPlay

- C:\rtpplay>rtpplay ?
- Usage: rtpplay [-v] [-T] [-p profile] [-f file] [-b begin time] [-e end time] destination/port[/ttl]
- -T uses the arrival time of packets
- -f rtpdump file name
- Destination/port
- Example rtpplay -T -f stream1 10.66.90.3/16542

# RTPPlay

- RTPPlay works with files in rtpdump format
- Use Ethereal to extract the problem stream  
“Statistics -> RTP -> Show All Streams...”



## How to playback the stream using RTPPlay

1. Get a call up from an IP phone to the device you wish to send the stream (phone or gateway)
2. Browse to the initiating phone and check the stream statistic and located the opened port of the receiving device
3. Unplug the initiating phone
4. Run RTPplay and send the stream to the IP/Port found in step 2



# Video Example of RTPplay



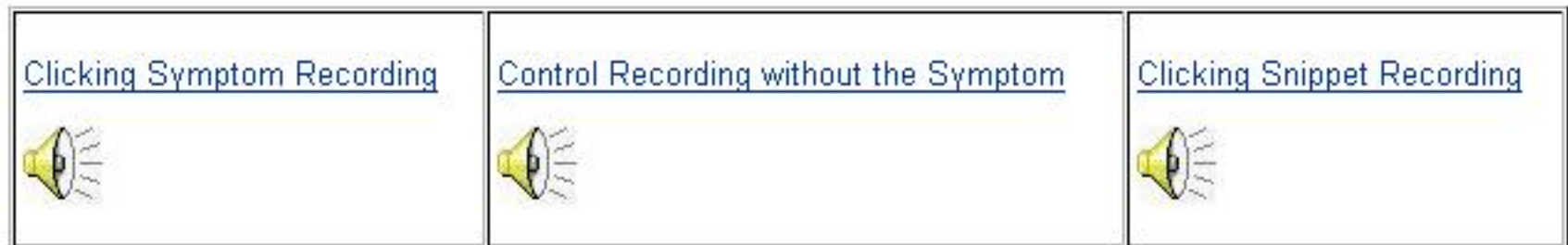
# Voice Quality Problems – Samples on CCO

- [http://www.cisco.com/en/US/tech/tk652/tk698/technologies\\_white\\_paper09186a00801545e4.shtml](http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00801545e4.shtml)

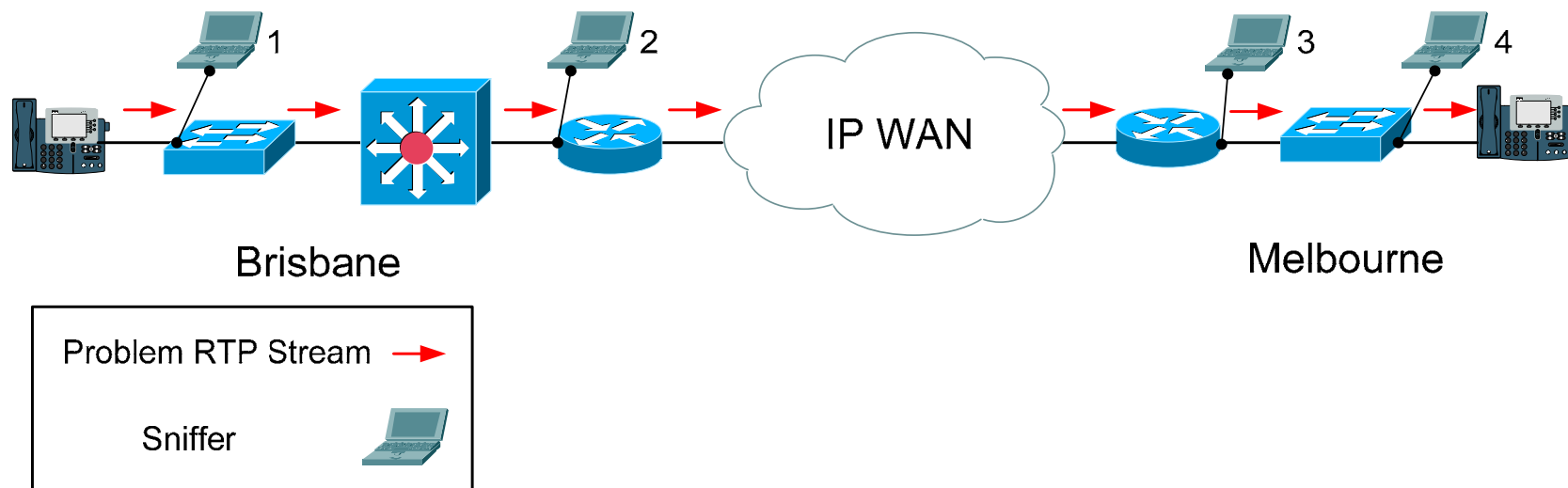
## Clicking

Symptom—Clicking is an external sound similar to a knock that is inserted usually at intervals.

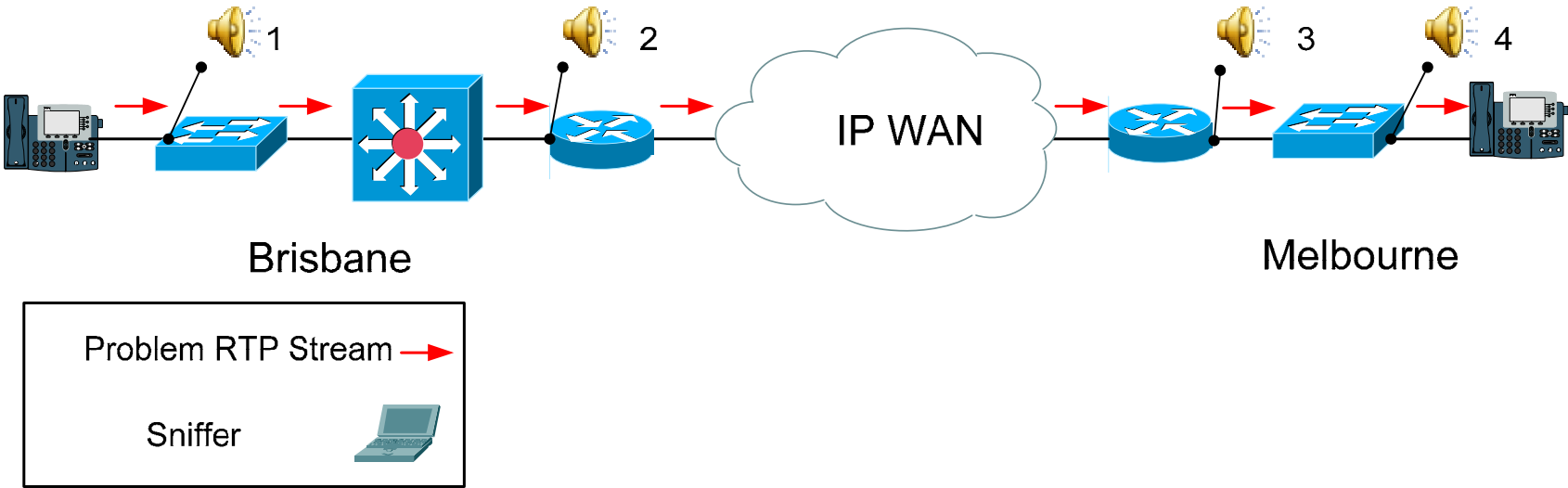
Cause—A common cause is clock slips or other digital errors.



# Back to our problem - Call Flow Diagram



# RTP Quality Capture



# Queuing Configuration

- class-map match-any signal
- match ip dscp cs3
- match ip dscp af31
- class-map match-all voice
- match ip dscp ef
- !
- policy-map Melbourne
- class voice
- priority 100
- class signal
- bandwidth 10
- class class-default
- fair-queue

# Queuing Statistics

- Rack02R1#show policy-map interface serial0/0
- Class-map: voice (match-any)
  - 9217 packets, 2244988 bytes
  - 30 second offered rate 231000 bps, drop rate 203000 bps
  - Match: ip dscp ef (46)
    - 9217 packets, 2244988 bytes
    - 30 second rate 231000 bps
  - Queueing
    - Strict Priority
    - Output Queue: Conversation 264
    - Bandwidth 128 (kbps) Burst 3200 (Bytes)
    - (pkts matched/bytes matched) 9217/2244988
    - (total drops/bytes drops) 6110/2041220

# Why are there Packet drops?

- Check configuration router configuration to ensure we are matching the correct traffic
- Confirm Call Manager Location settings
- Debug on the router with different access list to track the unknown traffic
- Sniffer trace capture all trace going into the router (wait! We have this already)

# Sniffer trace revisit

Ethereal: RTP Streams

Detected 13 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
142.102.64.11	29154	142.102.65.10	24568	2356583262	ITU-T G.729	914	0 (0.0%)	20.91	0.47	0.21	
142.2.64.11	24914	239.11.1.64	16392	1807	ITU-T G.711 PCMU	2856	0 (0.0%)	22.68	2.30	1.26	X
142.2.64.11	24922	239.11.1.64	16396	1811	ITU-T G.729	2856	0 (0.0%)	22.62	2.42	1.36	X
142.2.64.11	24926	239.11.1.64	16398	1813	Sun CellB video encc	2856	0 (0.0%)	22.24	8.70	8.22	X
142.2.64.11	24934	239.11.1.64	16402	1817	ITU-T G.711 PCMA	2856	0 (0.0%)	22.24	2.76	1.67	X
142.2.64.11	24938	239.11.1.64	16404	1819	ITU-T G.729	2856	0 (0.0%)	22.13	2.88	1.77	X
142.2.64.11	24898	239.11.1.64	16384	1799	ITU-T G.711 PCMU	2855	0 (0.0%)	23.01	2.15	1.01	X
142.2.64.11	24910	239.11.1.64	16390	1805	Sun CellB video encc	2855	0 (0.0%)	22.76	8.67	8.22	X
142.2.64.11	24902	239.11.1.64	16386	1801	ITU-T G.711 PCMA	2855	0 (0.0%)	23.12	3.14	0.93	X
142.2.64.11	24906	239.11.1.64	16388	1803	ITU-T G.729	2854	0 (0.0%)	22.99	3.25	1.01	X
142.2.64.11	24918	239.11.1.64	16394	1809	ITU-T G.711 PCMA	2854	0 (0.0%)	22.77	3.36	1.18	X
142.2.64.11	24930	239.11.1.64	16400	1815	ITU-T G.711 PCMU	2854	0 (0.0%)	22.66	3.48	1.30	X
142.2.64.11	24942	239.11.1.64	16406	1821	Sun CellB video encc	2854	0 (0.0%)	22.39	8.93	8.22	X

Select a forward stream with left mouse button  
Select a reverse stream with SHIFT + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

**Hold on! What's this?**



# MOH Settings

## Multicast Audio Source Information

Enable Multicast Audio Sources on this MOH Server

Base Multicast IP Address

Base Multicast Port Number  (Even numbers only)

Increment Multicast on  Port Number  IP Address

## Selected Multicast Audio Sources

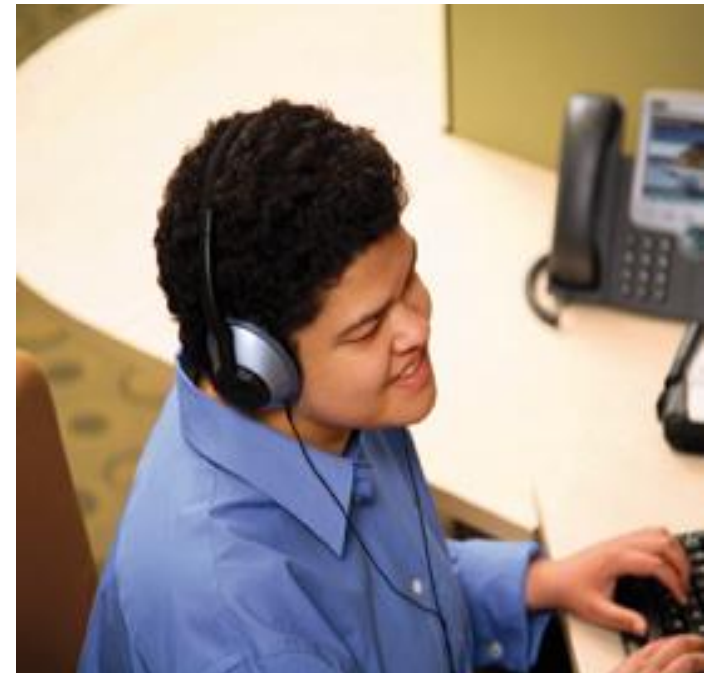
No.	Audio Source Name	Max Hops
1	SampleAudioSource	<input type="text" value="5"/>
2	Sales	<input type="text" value="2"/>
3	Marketing	<input type="text" value="2"/>

## Parameter Name

## Parameter Value

Supported MOH Codecs\*

711 mulaw  
711 alaw  
729 Annex A



# SRND Reference to Multicast MOH Setup

- From Solution Reference Network Design 4.x
- [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guide\\_chapter09186a00806e8c28.html#wp1043734](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a00806e8c28.html#wp1043734)
- “IP network routers route multicast based on IP addresses, not port numbers. “

# Summary

- Identify Call Manager Call Flow
- Trace Reading Tools
- Sniffer Capture Decoding Tools
- Sound Quality Analysis



# Q and A



