It's Not the Network!
The Value of Root Cause Analysis

Graeme Bailey

Troubleshooter

TARCA

TROUBLESHOOTING & ROOT CAUSE ANALYSIS

@TARCAtools

What is this session?

It is not

- How to use Wireshark
  - Laura and Betty are much better at that than I am
- How to decode TCP etc.
- Why you should be using IPv6

It is

- A collection of real experiences
  - I have the pcap files etc.
- An insight into how I approach troubleshooting a problem
  - Some of my customers say my brain is just wired differently
- Hopefully going to inspire a few people to think about more than just the network and consider the big picture

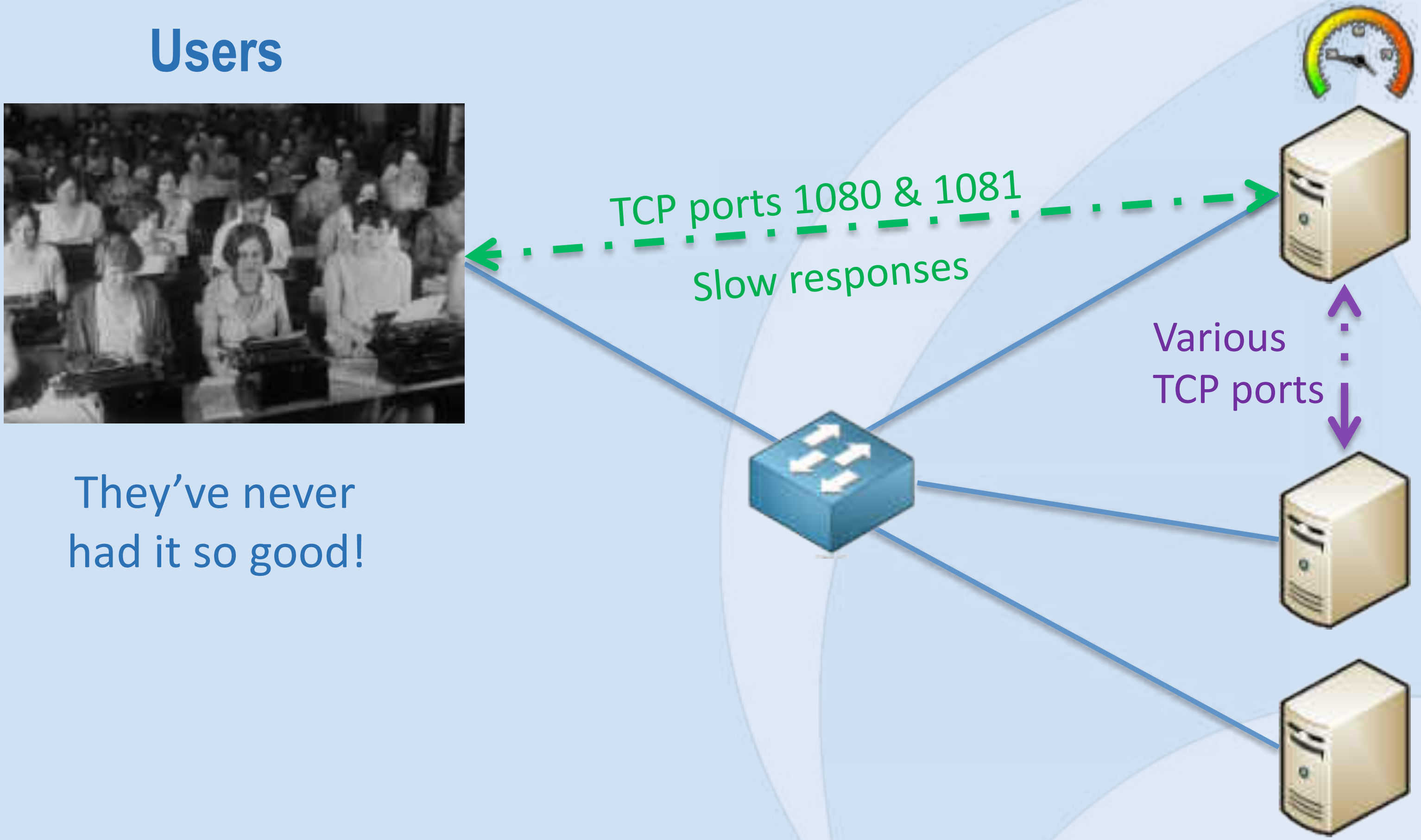
White Screen, it's Frozen!

Well that's what the users reported!

What are the symptoms?

- Opening/saving documents sometimes takes 30 to 200 seconds or occasionally hangs completely
  - 10’s of minutes lost per user per day
    - Should only take a few seconds
- General time wasted
- Lost billable minutes
- Deadlines missed

What’s going on?



Users

They’ve never
had it so good!

TCP ports 1080 & 1081

Slow responses

Process
CPU %
Memory
User CPU %

DMS
Servers

Various
TCP ports

TCP TDS
No slow
responses
Waffle!

SQL
Servers

File
Server

SHARKFEST ‘12

What should we learn from this?

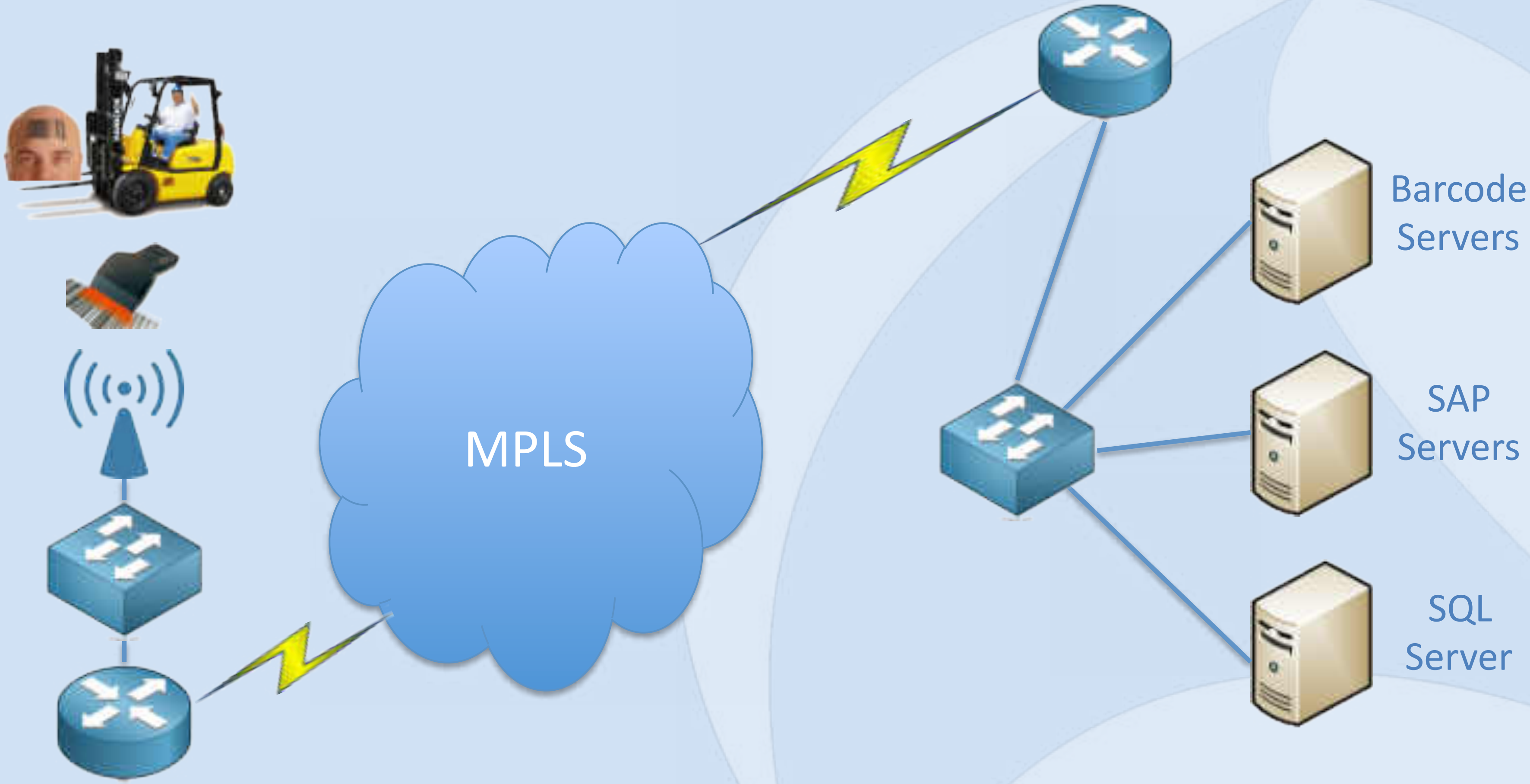
- Double check what the users are reporting
- Just because a server isn’t 100% CPU doesn’t mean it isn’t busy
- Correlate data to user issues
- Users not complaining doesn’t equal no problems
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Stand your ground

We’re not making Pop!

What’s the symptom?

- 14 minutes to transfer a pallet to warehouse rack
  - Over 9 hours to unload each lorry (truck)
    - Should take 1 hour or less
- Shortage of raw materials resulted in production being suspended!

What’s going on?



What should we learn from this?

- Double check what the users are reporting
- Process of elimination
- Use detail data to follow the transaction
- Work through the tiers (sometimes tears)
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Validate the resolution

Everything's slow, it must be the Network!

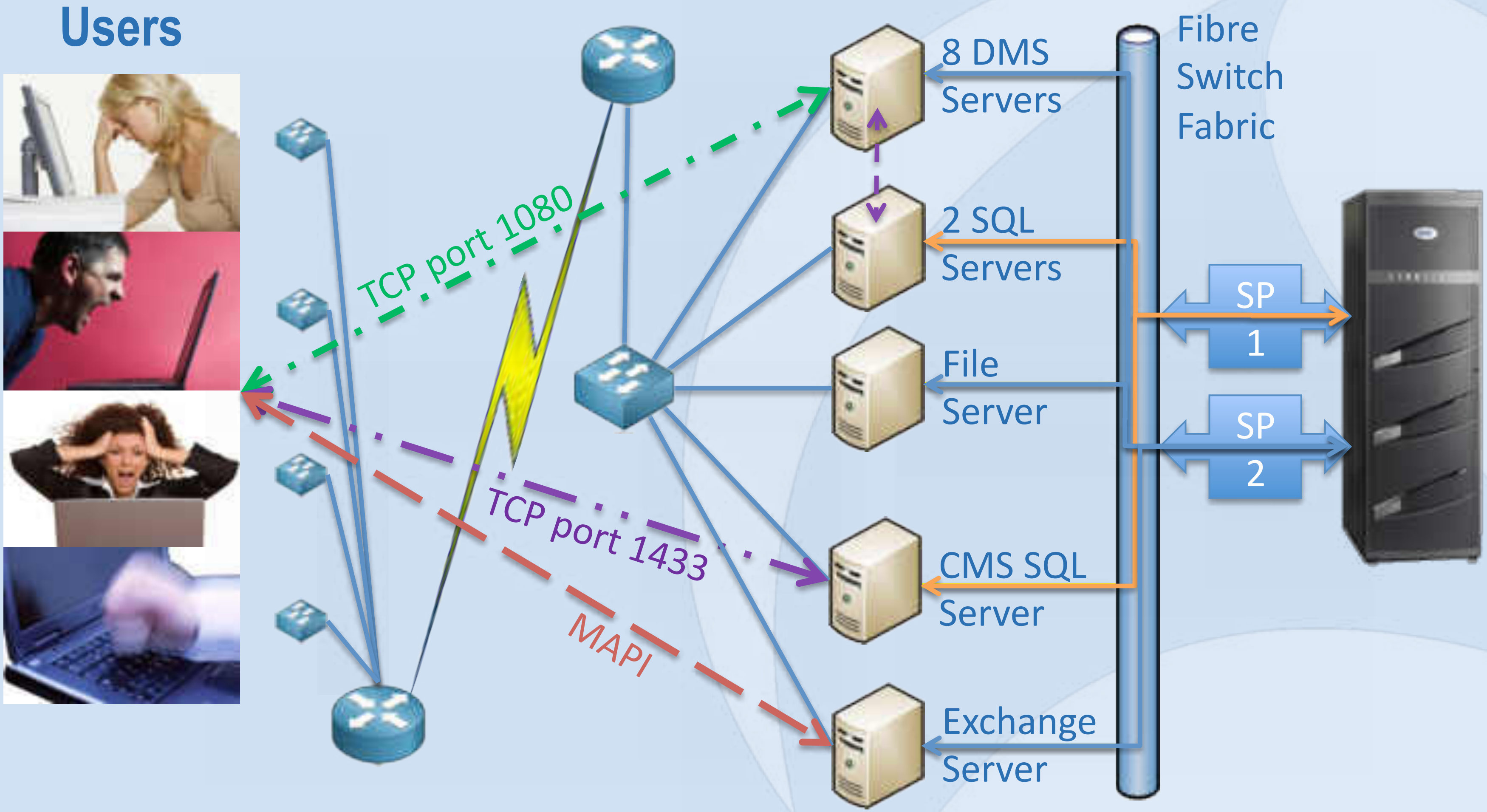
CACE Technologies Presents:
The Case of the Slow Network
WIRESHARK
DETECTIVE AGENCY
NETWORK MYSTERIES SOLVED BY CACE PILOT AND WIRESHARK

A little bit of history!

What are the symptoms?

- Intermittently, multiple mission critical applications all running slowly at the same time
  - Document management system (DMS)
  - Case management system (CMS)
- 1,000+ users in London HQ, servers in remote DC
  - Different applications running on different servers, so it must be the network link to the DC, mustn't it!
  - Network monitoring systems show no problems

What's going on?



What should we learn from this?

- Double check what the users are reporting
- Process of elimination
- Correlate data to follow the transaction
- Work through the tiers (sometimes tears)
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Validate the resolution

It's a web application so it must be OK over the WAN!

They're thin, light, elegant and efficient.
No, you're thinking of a spider's web!

What are the symptoms?

- Intranet apps respond slowly, especially over low bandwidth and/or high latency WAN links
- Theoretically, browser based apps ‘should’ be suitable to run over WANs as they ‘should’ be suitable to run over the internet
  - – Only if they’ve been written well, and many aren’t
  - – Too many elements and large content are common
- SharePoint - enough said?

‘It’s fine in HQ’

- Remote sites complain about slow responses
  - We’ve increased the bandwidth and it’s no better
- Latency
  - How many elements are on the page?
  - How many HTTP requests for the page?
  - Multiple versions of icons!

‘That’s a pretty web page’

- Remote site complains of slow Outlook until 09:30
  - We should increase the bandwidth, shouldn’t we?
- **Health Warning**

‘Allowing users to control web content is hazardous to your network’s health and can be fatal’

- What do they do that’s so bad?
  - That’s a nice picture, we need high resolution!
  - So if you scroll down a few pages you’ll find it!

‘We’ve implemented SharePoint’

- Intranet home page load time is now 3 to 8 seconds
  - The old site could only manage 300mS
- What’s it doing?
  - Is the authentication configured properly?
  - What servers is it accessing to deliver content?
  - How did they load test it?
    - Realistic content
    - Caching

A nice little SQL request

```sql
SELECT TOP 2147483648 t1.[Type] AS c0,UserData.[ntext2],UserData.[datetime1],t2.[tp_ID] AS c5c7,UserData.[ntext7],UserData.[tp_ItemOrder],t1.[TimeLastModified] AS c15,UserData.[tp_Created],UserData.[tp_ModerationStatus],UserData.[nvarchar1],UserData.[bit2],t3.[nvarchar1] AS c11c6,UserData.[tp_WorkflowInstanceID],t1.[Id] AS c3,UserData.[ntext1],t3.[tp_Created] AS c11c10,t1.[MetaInfo] AS c2,UserData.[ntext6],UserData.[bit4],UserData.[tp_Modified],t2.[nvarchar5] AS c5c9,UserData.[tp_UIVersion],UserData.[tp_ID],UserData.[tp_CopySource],UserData.[ntext3],UserData.[bit1],UserData.[sql_variant2],UserData.[datetime2],t2.[tp_Created] AS c5c10,t3.[nvarchar5] AS c11c9,t1.[TimeCreated] AS c13,UserData.[tp_InstanceID],UserData.[tp_GUID],CASE WHEN DATALENGTH(t1.DirName) = 0 THEN t1.LeafName WHEN DATALENGTH(t1.LeafName) = 0 THEN t1.DirName ELSE t1.DirName + N'/' + t1.LeafName END  AS c1,UserData.[tp_Author],t2.[nvarchar4] AS c5c8,UserData.[tp_Editor],t3.[nvarchar4] AS c11c8,UserData.[tp_UIVersionString],t1.[LeafName] AS c12,UserData.[nvarchar2],UserData.[ntext5],UserData.[bit3],UserData.[tp_ContentType],UserData.[tp_ContentTypeId],UserData.[sql_variant1],t3.[tp_ID] AS c11c7,UserData.[tp_WorkflowVersion],t1.[ProgId] AS c16,UserData.[tp_Version],t1.[ScopeId] AS c4,UserData.[tp_IsCurrentVersion],UserData.[tp_HasCopyDestinations],UserData.[tp_Level],UserData.[ntext4],t2.[nvarchar1] AS c5c6,UserData.[tp_HasAttachment],t1.[DirName] AS c14 FROM UserData  LEFT OUTER LOOP  JOIN Docs AS t1 WITH(NOLOCK) ON ( 1 = 1  AND UserData.[tp_RowOrdinal] = 0 AND t1.SiteId = UserData.tp_SiteId AND t1.SiteId = @L2 AND t1.DirName = UserData.tp_DirName  AND t1.LeafName = UserData.tp_LeafName AND t1.Level = UserData.tp_Level  AND t1.IsCurrentVersion = 1 AND (1 = 1)) LEFT OUTER JOIN AllUserData AS t2 WITH(NOLOCK, INDEX=AllUserData_PK) ON (UserData.[tp_Author]=t2.[tp_ID] AND UserData.[tp_RowOrdinal] = 0 AND t2.[tp_RowOrdinal] = 0 AND ( (t2.tp_IsCurrent = 1) )  AND t2.[tp_CalculatedVersion] = 0  AND t2.[tp_DeleteTransactionId] = 0x AND t2.tp_ListId = @L3 AND UserData.tp_ListId = @L4) LEFT OUTER JOIN AllUserData AS t3 WITH(NOLOCK, INDEX=AllUserData_PK) ON (UserData.[tp_Editor]=t3.[tp_ID] AND UserData.[tp_RowOrdinal] = 0 AND t3.[tp_RowOrdinal] = 0 AND ( (t3.tp_IsCurrent = 1) )  AND t3.[tp_CalculatedVersion] = 0  AND t3.[tp_DeleteTransactionId] = 0x  AND t3.tp_ListId = @L3 AND UserData.tp_ListId = @L4) WHERE  UserData.tp_ListID=@L4 AND ( (UserData.tp_IsCurrent = 1) )  AND UserData.tp_SiteId=@L2 AND (UserData.tp_DirName=@DN OR UserData.tp_DirName LIKE @DNEL+N'/%') AND UserData.tp_RowOrdinal=0 AND (t1.SiteId=@L2 AND (t1.DirName=@DN OR t1.DirName LIKE @DNEL+N'/%') AND t1.Type=0) ORDER BY UserData.[tp_ID] Asc OPTION (FORCE ORDER)
```

What should we learn from this?

- Web doesn’t necessarily mean thin
- Understand how the app delivers the content
- Correlate data to follow the transaction
- Work through the tiers (sometimes tears)
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Validate the resolution

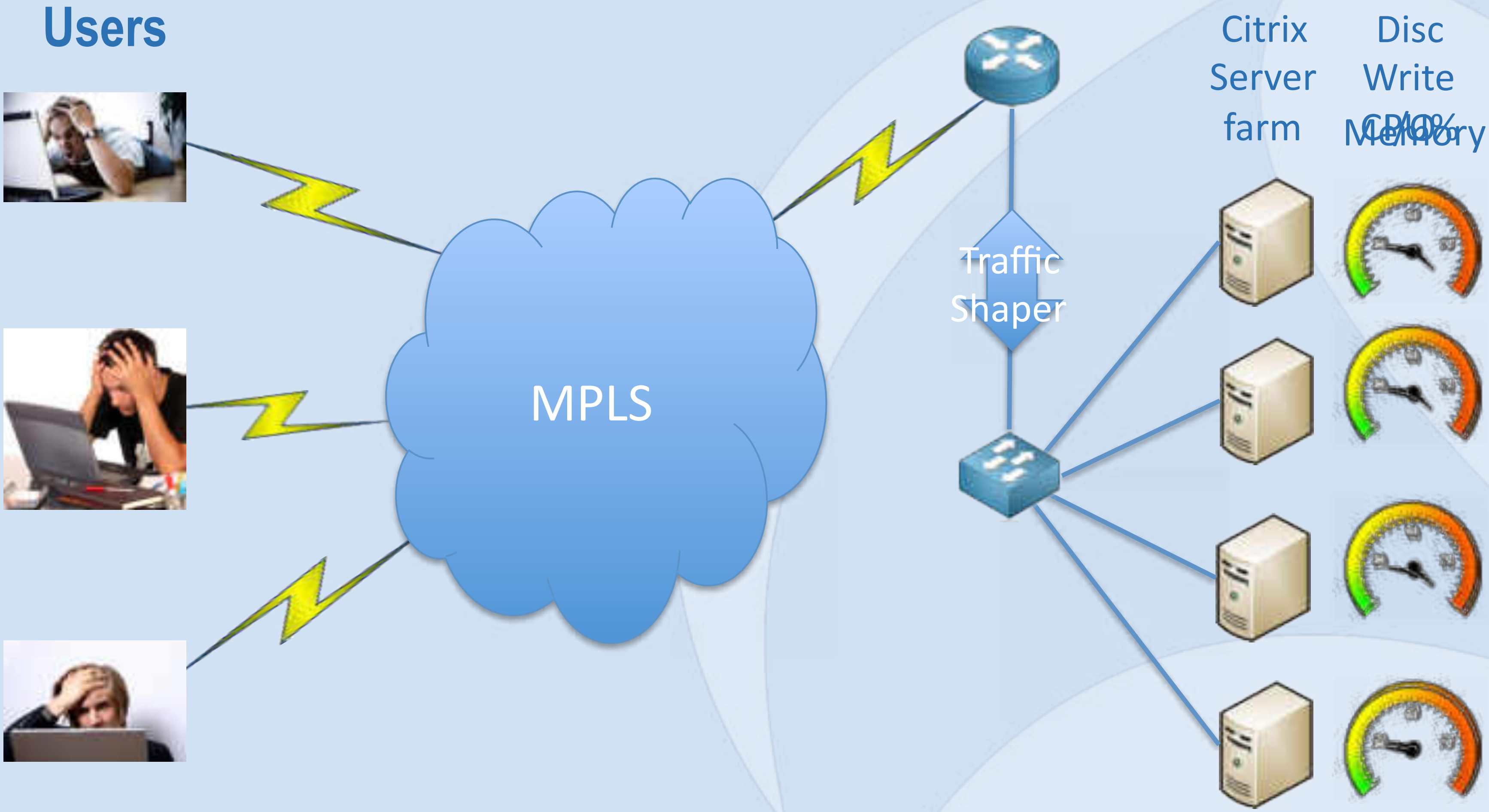
Typing L............ag!

Don't you just hate it when the letters stick?

What are the symptoms?

- Citrix users complaining of typing lag, jerky and erratic scrolling of documents
- Sessions hanging, slow to respond

What’s going on?



Users

MPLS

Traffic Shaper

Citrix Server farm

Disc Write

CPU0%

Memory

What should we learn from this?

- Sometimes it is the network
- Many different causes, same user symptom
- Check the full End-to-End path
- Anything in the network can cause problems
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Validate the resolution

What can you take with you?

- Keep an open mind
- Think about the big picture
- Users are just another source of data (unreliable?)
- Think about what is happening low down
- Process of elimination
- Often multiple little issues equal one big one
- Double check your data and understanding
- Keep your mouth shut until you are certain
- Don’t give up!
- If your brain is wired differently, count yourself lucky!

SHARKFEST '12

Wireshark Developer and User Conference

Graeme Bailey

Troubleshooter

TARCA
TROUBLESHOOTING & ROOT CAUSE ANALYSIS

TARCA tools
TROUBLESHOOTING & ROOT CAUSE ANALYSIS

www.tarca.co.uk

www.tarcatools.com

www.facebook.com/TARCAtools

www.tarcatools.wordpress.com

@TARCAtools