



**Frontline Network Troubleshooting
Success Strategies**



Agenda

- Organizational Factors & Self Evaluation
- Success Strategies for Frontline Troubleshooting
- Case Study



Your presenter:

Dan Klimke

Marketing Manager, Network Tools

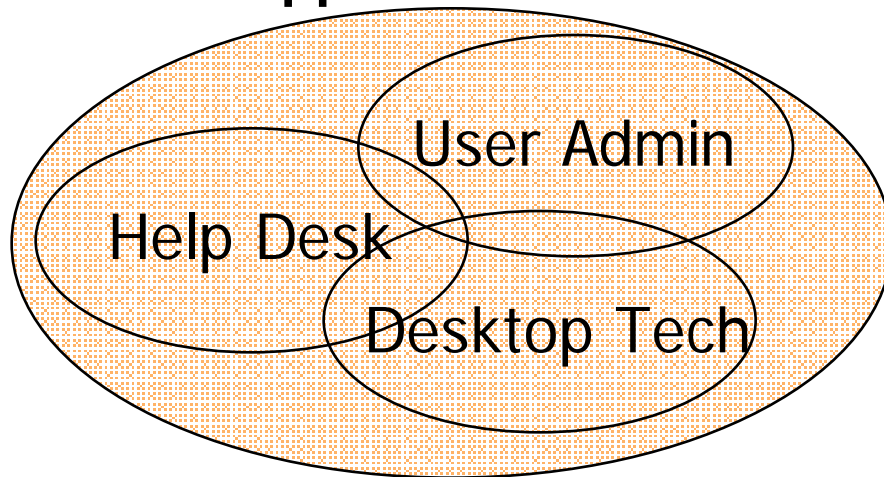
Fluke Networks

dan.klimke@flukenetworks.com



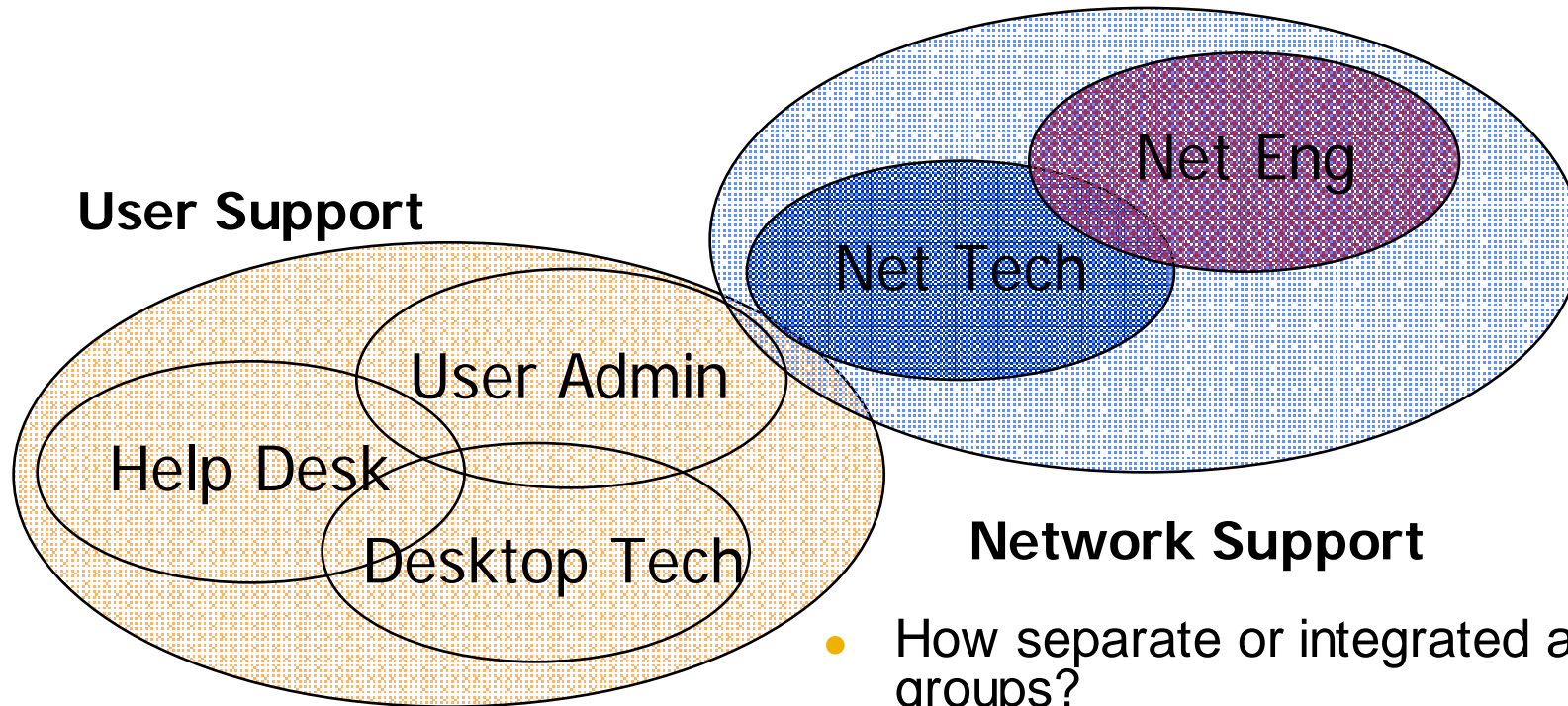
What does your organization look like?

User Support





What does your organization look like?

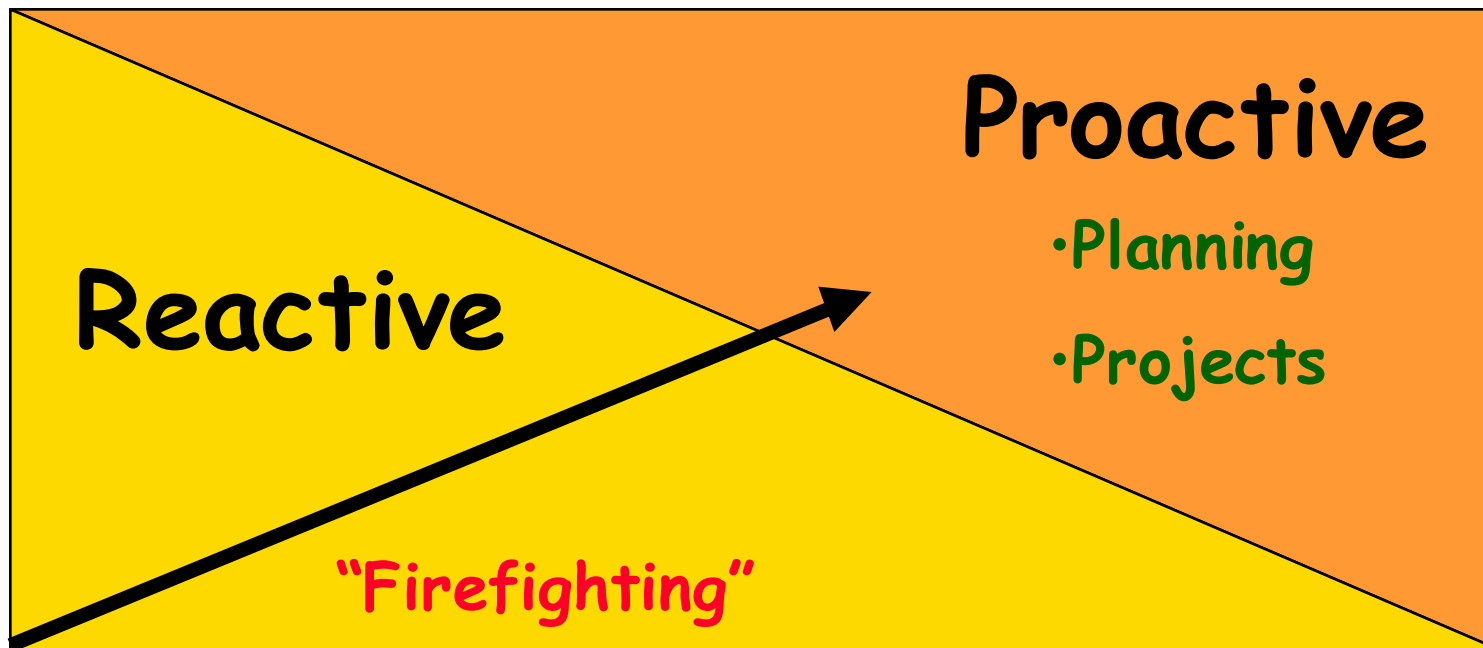


Network Support

- How separate or integrated are these groups?
- How freely is information exchanged?
- Do each know and understand the objectives and priorities of the other?



Everyone wants to be more proactive...
Where do you fit on the scale?



Is your time being spent where it should be?



What is in place right now?

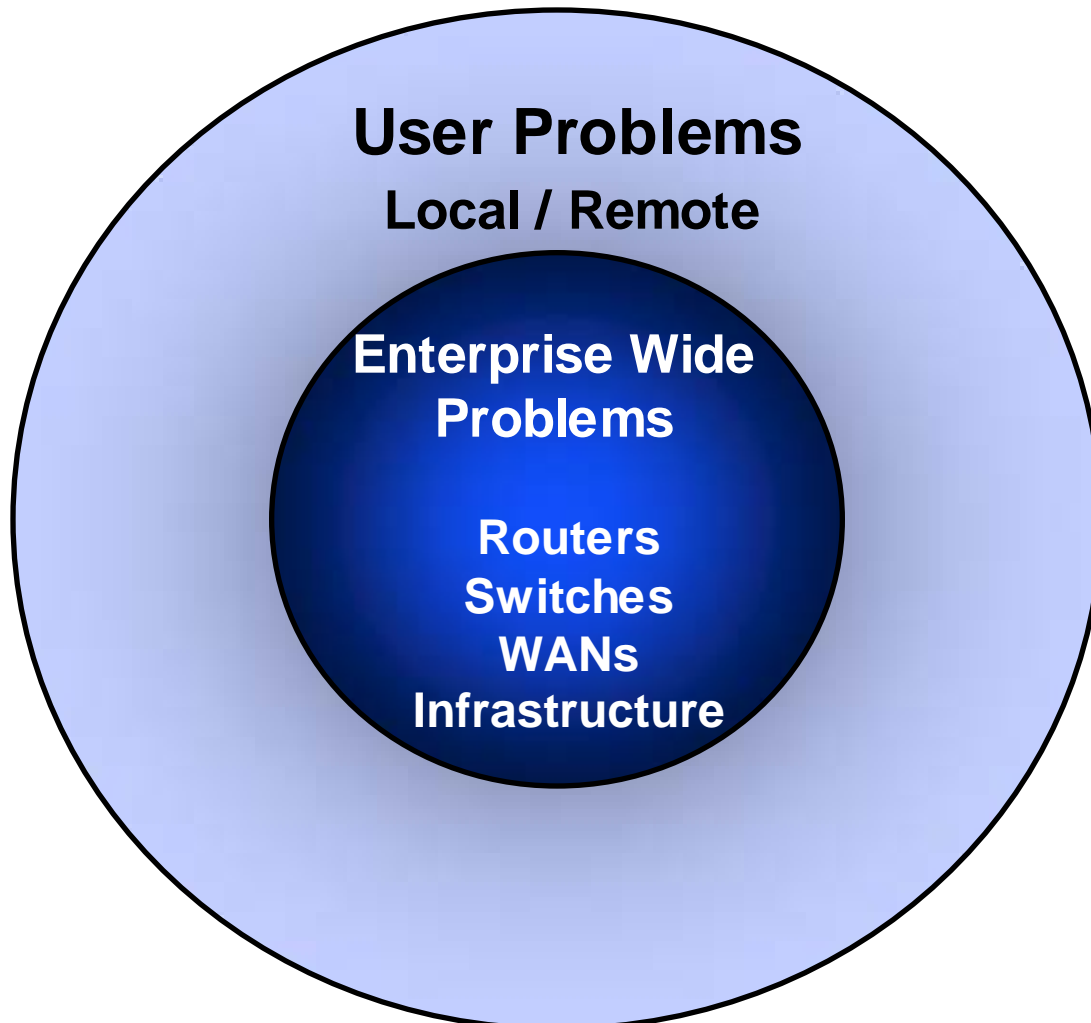
- Documentation?
- Baselines?

What's "normal" on your network?

- Flowcharts / process maps?
- Standards?



Network Problems



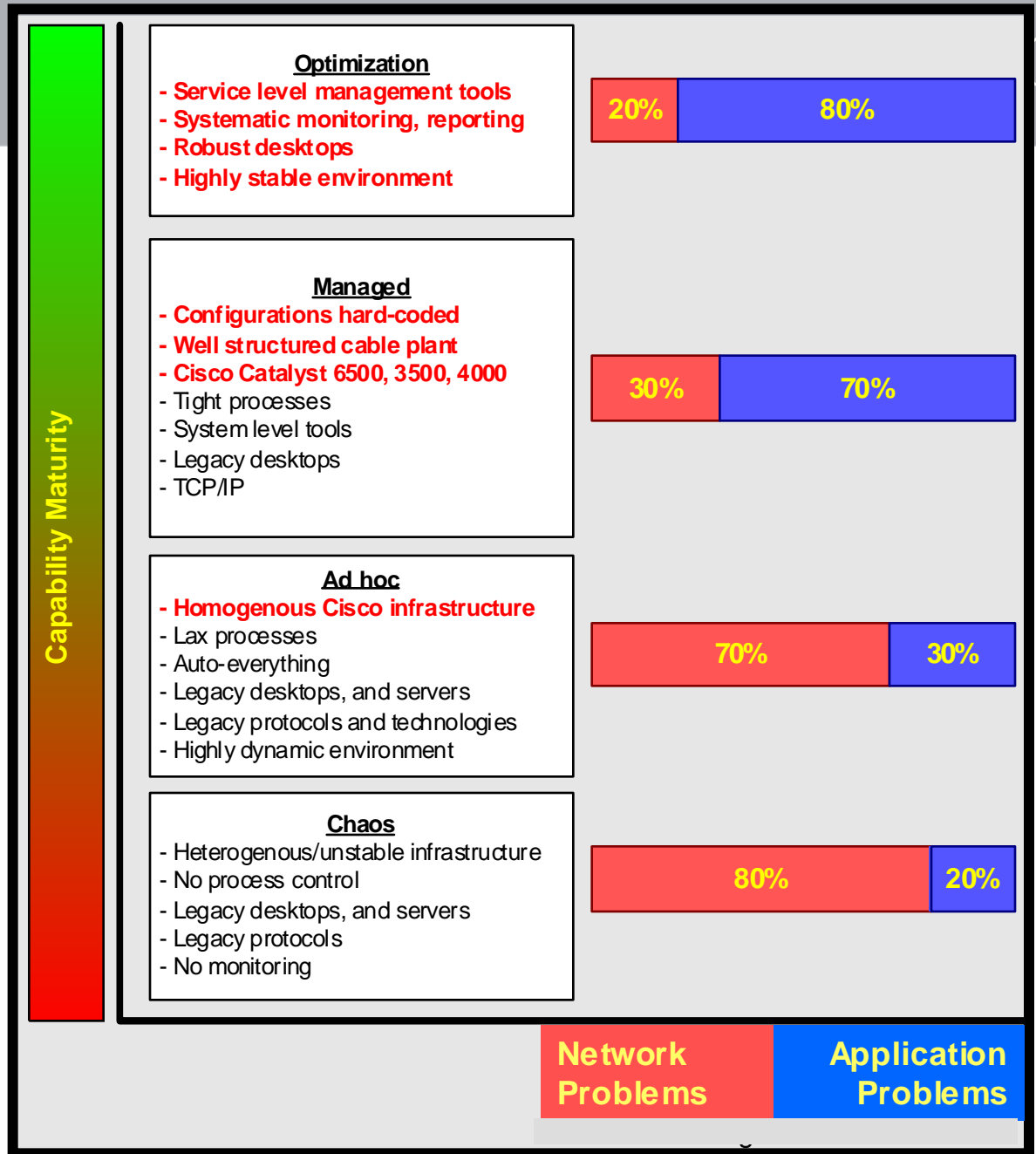
User Problems

- Large in number
- Each has small impact on network
- Collectively have large impact on user support organization
- Need to be resolved at front line by techs with typically less experience and few tools

Network/Enterprise Wide Problems

- Small in number
- Affect many users and locations
- Requires high-level expertise and expensive tools

Network Capability Maturity Model





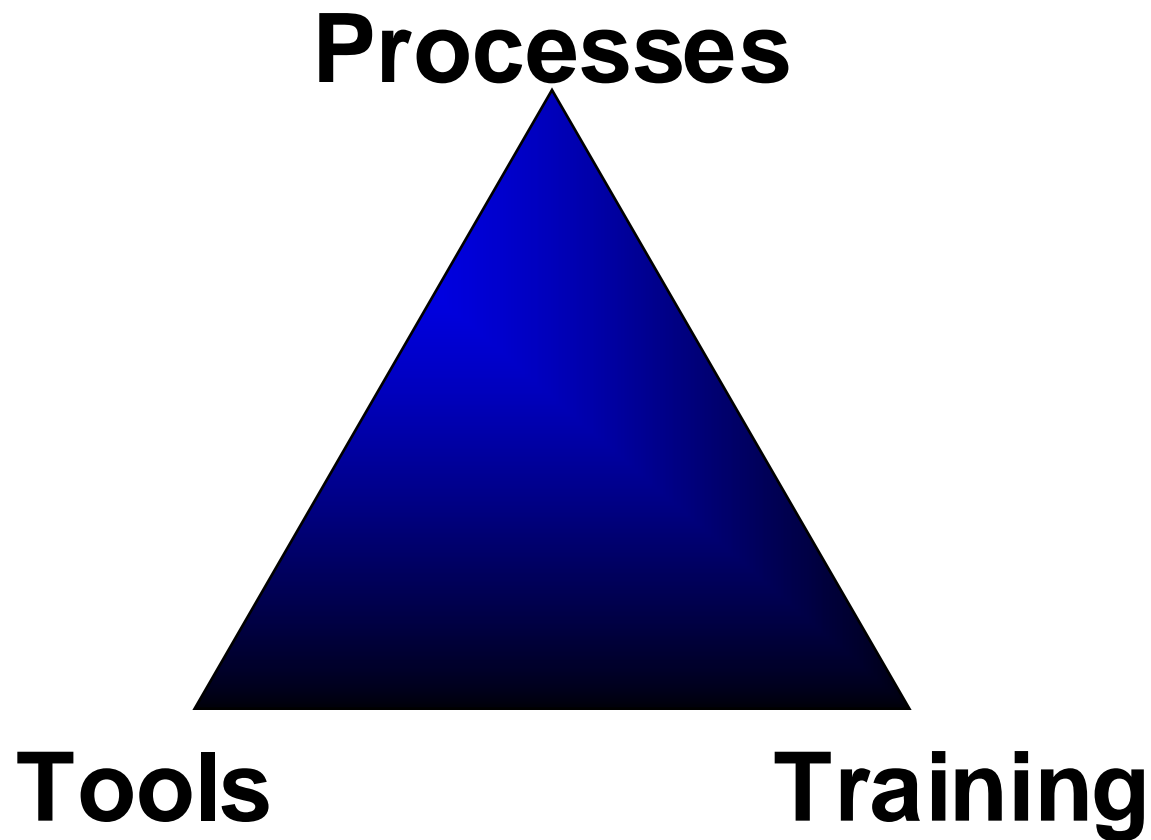
So, What Common Frontline Problems or Tasks Do You Face?

- “I can’t print”
- “I can’t get to the web”
- “I can’t login”
- “The network/app is slow”
- Moves, Adds, Changes
- Provisioning new drops

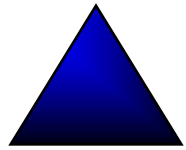
**How can you
solve them?**



The Keys to Success

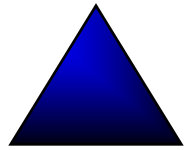


NETWORKSUPERVISION



Best Practices - Processes

1. Preparation and Planning
2. Problem Prevention
3. Early Problem Detection
4. Fast Problem Resolution



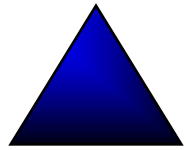
Best Practices - Processes

- **1 - Preparation & Planning**

Standards

Documentation & Baselines

Have a Documented Plan - what, who, and how



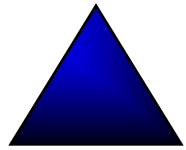
Best Practices - Processes

2 - Problem Prevention

Prevent problems before they happen

Do's and Don'ts for End Users

Testing and Certification



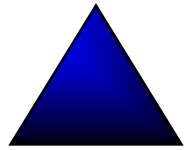
Best Practices - Processes

- **3 - Early Problem Detection**

Network Monitoring

Periodic Audits (update baselines)

Centralized Help Desk w/Trouble-ticketing system



Best Practices - Processes

4 – Fast problem resolution

Follow a troubleshooting methodology!

- Step 1. Collect Information
- Step 2. Localize & Isolate the Problem
- Step 3. Correct the Problem
- Step 4. Verify Problem Resolution
- Step 5. Document What You Did



Step 1. Collect Information

- Understand the problem
 - have the user demonstrate the problem to verify it.
- Was something changed before it occurred?
 - Will users confess?
- Assume nothing.
 - No they won't! Or, they may not realize what they've done could affect the network.
- Did it ever work before?
 - If no, treat that situation like a new installation
 - If it did, then troubleshoot it.



Step 2. Localize and Isolate the Problem aka: Divide and Conquer

- Is the problem...
 - Network-wide?
 - Localized to a single segment?
 - On a single station?
 - Affecting only one account?
- Reducing the scope of the problem in this way is where divide-and-conquer begins.
- Be a “SLI” troubleshooter!
 - Segment, Localize, Isolate



Step 2. Isolate the Problem - Network Segment

- Any “rogue hubs” out there?
- Turn off or disconnect all but two stations
Realistic? Not really...
- Once those two are communicating, add more stations.
- If they are not communicating, check the physical layer possibilities such as the termination of the cable, the cable itself, or the segment’s hub.
- ALWAYS suspect the physical layer FIRST!



Step 2. Isolate the Problem - Single Stations

Isolate the problem to

- Specific hardware
 - NIC, HUB/Switch Port, Cable, Patch Cords
- Account Settings
 - user's network account, security and permissions
 - compare account to one that works
- Software



Step 3. Correct the Problem

Once a single operation, application or connection is localized as the source of the problem, identifying the specific fault *should* be simple.

- Single station problems:

- Test then replace network adapter

- Try a fresh copy of the network driver software

- New network/patch cable

- Compare configurations with another workstation

- Reinstall the problem application.

- Do not trust any existing configuration file.



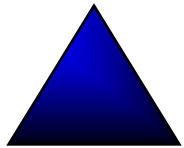
Step 4. Verify Problem Resolution

- Have the user test for the problem. Also, have the user try several different operations with the equipment.
- Sometimes a repair in one area causes other problems, and sometimes whatever was repaired turns out to be a symptom of another underlying problem.



Step 5. Document

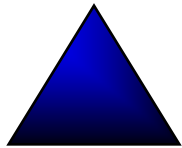
- Document what you did.
- Document what you did.
- Document what you did.



Best Practices - Tools

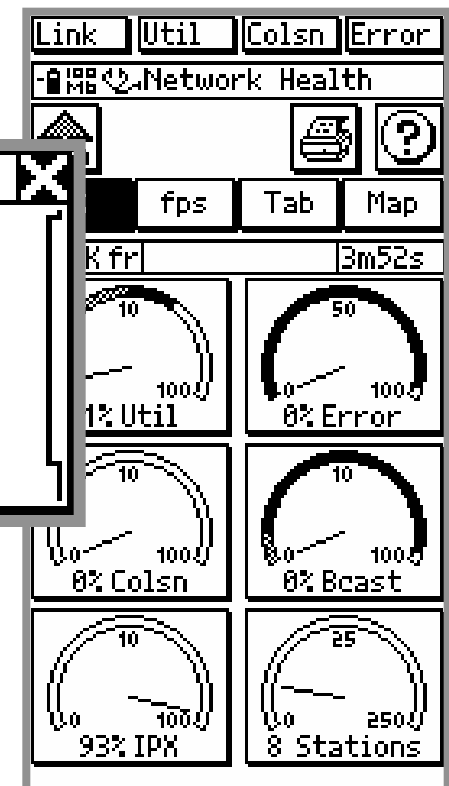
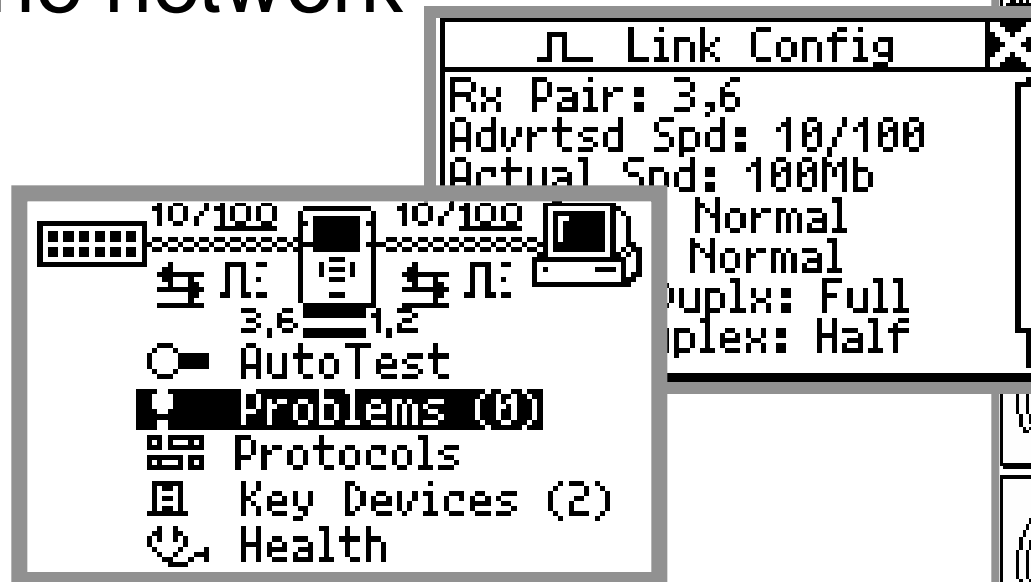
- Invest in labor and time-saving tools rather than additional staff to deliver network performance
 - “Right tool for the right person”
- Cut out guesswork
- Speed problem resolution



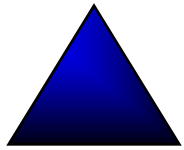


Best Practices - Tools

- Network test tools provide definitive information about the problem & what is going on in the network



NETWORK SUPERVISION

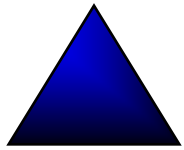


Best Practices - Tools

Cable Testers – there are two kinds:

- Basic Testers Should Find
 - Miswires
 - Opens, Shorts, Length
 - Split Pairs (this is important!)
- Cable Certification Tools Will Also
 - Measure Attenuation & NEXT
 - Determine Cable Performance
 - Find Crosstalk Faults





Best Practices - Tools

Protocol Analyzers – Software

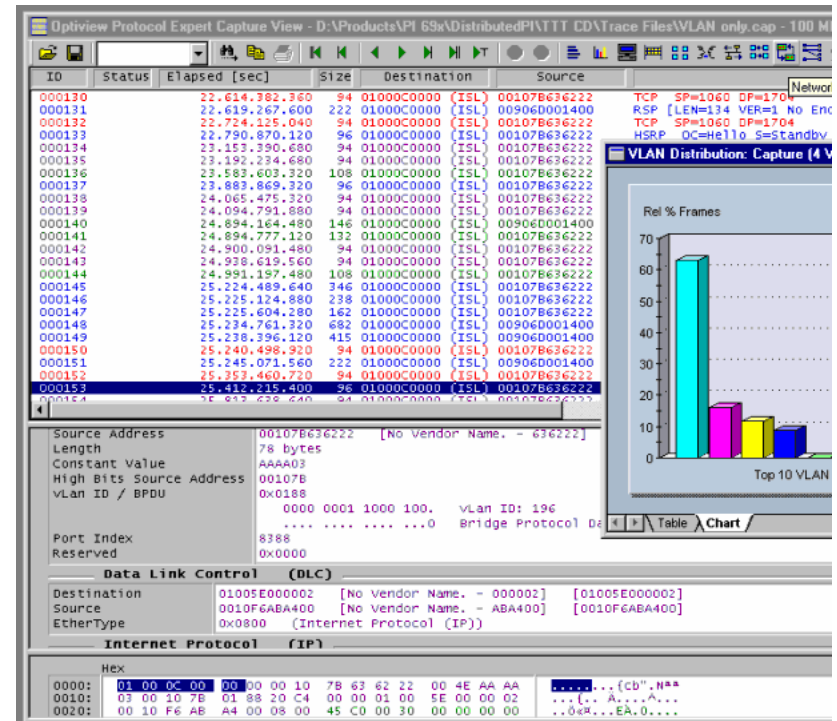
Many “freeware” analyzers out there

May ‘do the job’ for simple analysis

You get what you pay for

Higher-end analyzers include ‘experts’ to provide assisted troubleshooting.

Necessary for application-response troubleshooting





Problems in the “old days” of shared Ethernet:

- Collisions
- Errors
- Utilization
(Top Talkers / Receivers)
- Excessive Broadcasts

**Cause: Traffic
Pattern &
Hardware
Faults**

Protocol analyzers used to be effective in finding and solving these issues, but in today's switched networks, a protocol analyzer offers only limited visibility. We'll discuss why in a few slides...



Problems in today's switched Ethernet:

- “Can't connect”
Cable issues / Link ID
- Autonegotiation
Speed/Duplex mismatches
- Broadcast ‘storms’
Traffic related problems
- Slow Applications

- The common causes:**
- Failed equipment
 - Faulty drivers
 - Misconfiguration



When problems do occur, how can you solve them?

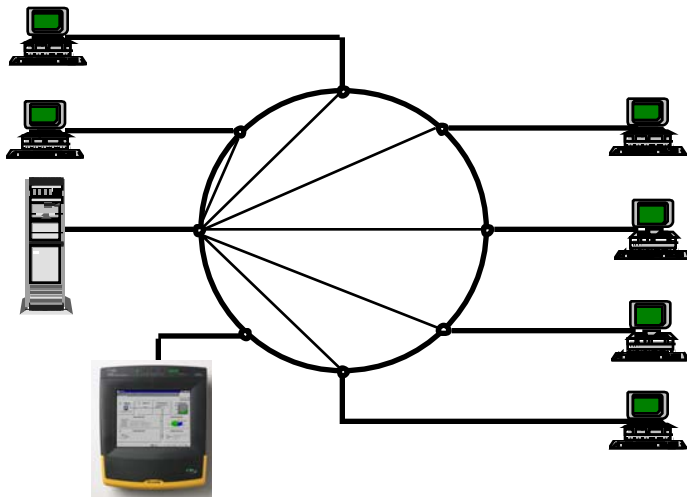
Common troubleshooting techniques:

- Ping to/from affected station/segment
- Remote access/control
- Check account configuration
- Got Link?
- Boot up admin laptop on link
- Swap Hardware
 - NIC, Hub, Patch Cords...



Visibility is the Single Biggest Problem in a Switched Environment

What traffic will a protocol analyzer see?



Mainly broadcast traffic!



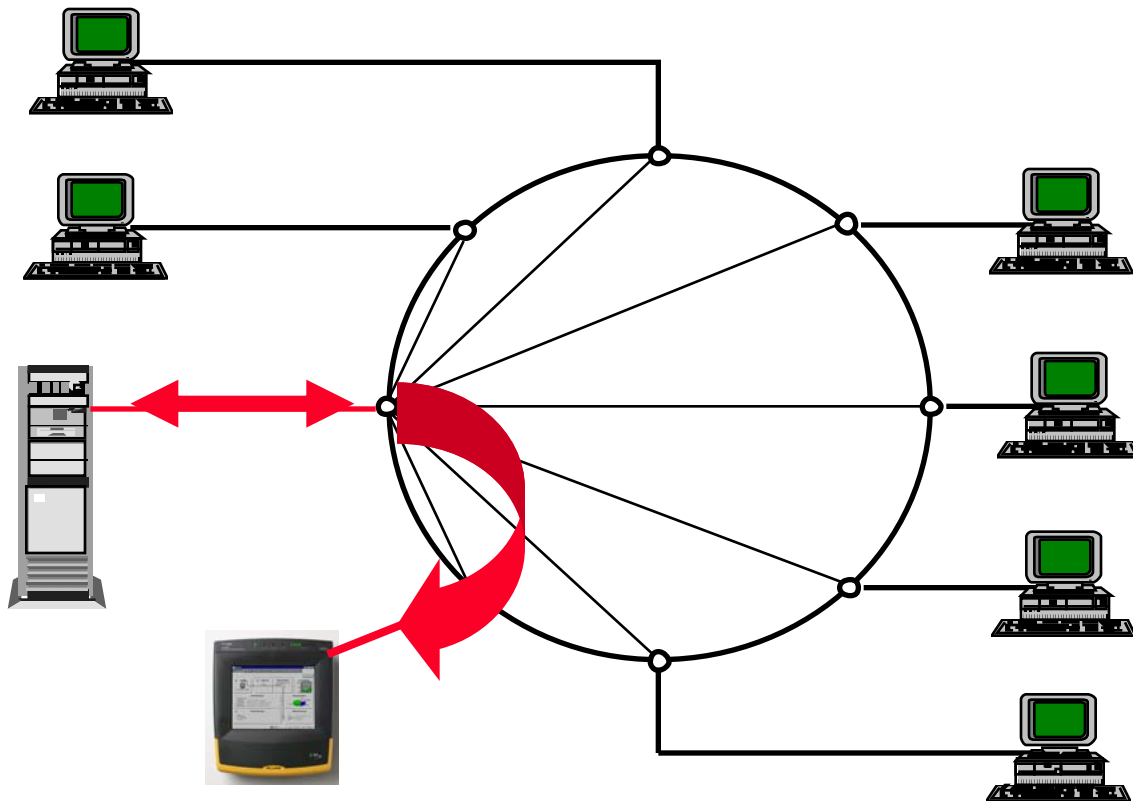
Port SPAN or Mirroring DOES allow you to see traffic to/from a single station.

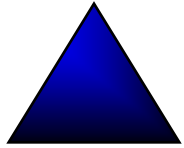
However:

The switch may not forward all traffic (dropped frames) and certainly will not forward errors.

Its performance may be affected by the act of spanning!

This is also a task that is not often delegated to the frontline tech





Best Practices - Training

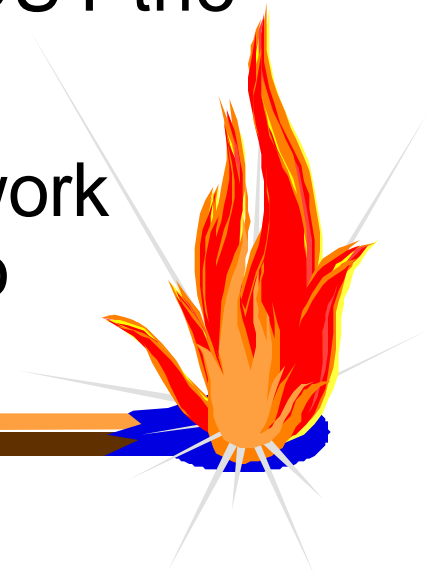
- Establish minimum standards, consistency
- Cross-training between groups
- Ensure purchased training is 'reality based'

Lab exercises on live networks



Analogy - Training

- Cities & Fire Departments spend tremendous effort, education, and dollars in PREVENTING FIRES
- But they also want and need the best possible equipment and trained staff to PUT OUT the FIRES when they DO occur.
- When you are in the middle of a network outage or slowdown is not the time to figure out how to use your analyzer!





Case Study

- High tech manufacturing company HQ
- Approx. 2,000 users over 4 sites nationwide
- Network in 'disarray'
- Symptoms:
 - Extended MTTR on trouble tickets
 - Fingerpointing between user support and network group
 - General lack of cooperation between groups
 - High user-dissatisfaction with IT in general



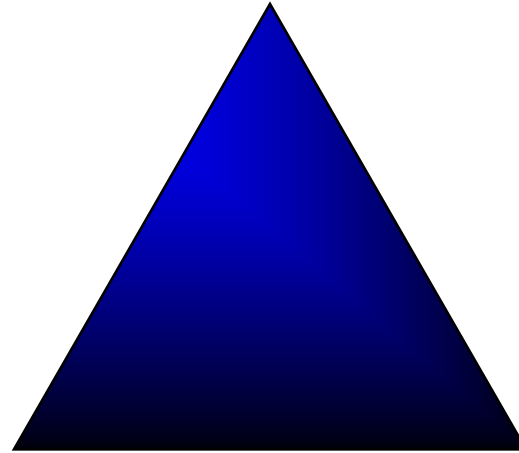
Solutions

- New IT manager!
- Used instance of upgrading network equipment to overhaul department processes, tools, training
- Network Support Staff & User Support Staff representatives attend each other's department meetings
- Network techs/engineers provide training to frontline staff
- Frontline staff equipped with basic test tools to speed problem resolution & limit false escalations
- Troubleshooting flow charts aid problem resolution
- Process diagrams and escalation procedures clearly indicate proper procedures & who is responsible for what



Remember the key success factors...

Processes



Tools

Training

Thank you for attending! Questions?