Shaking Your Network To Bits

Getting a Grip On Your Technology

info@thetechfirm.com

Agenda

Morning

- What The Heck Is a Tool?
- Urban Legends And Myths.
- Layer 2 And VLANS
- More Design Dilemmas
- What To Ask Yourself ?
- Is Your Network Built for Connectivity, Performance or Convenience?
- What Is The Network In “Network Management”?
- What About My Phone??

Lunch

- Tony’s Top Ten Customer Issues. (sort of)
- Client Misconfigurations
- Network Device Misconfigurations
- Server Misconfigurations
- Application Notes
- Sample Web Browsing Exercise
- The Lay Of The Land - Example

Room Protocols and Specifications

- Please set your pager or phone to ‘silent’ or vibrate mode.
- Do not save your questions for the end of the day, even if its off topic. Ask your questions when they pop into your head.
- There are no ‘*dumb questions’*.
- Don’t be afraid to ask ‘any’ question; even if you feel it is off topic.
- I always provide a morning and afternoon break along with lunch, but make sure to let me know if you feel you need a break.

What The Heck Is a Tool?

- Over the past 5 years or so, it seems that technicians who use true tools are quickly becoming extinct. More and more technical support staff are reaching for that '**pretty'** or **'automated tool'** that will make all their problems **magically** go away.
- Realties regarding tool use:
  - ✓ Data interpretation is typically a tedious/manual process.
  - ✓ A tool is the wrong hands is more dangerous than not having a tool at all.
  - ✓ It **WILL** take **MANY** tools to get a job done, not one favorite.
- If you pick up any tool without a clear objective, you're wasting your time.

Dice are NOT tools!

So put them back in the casino where they belong!!

Tools, The Drama

- Some technicians who purchase tools are very disappointed when they can't find a catastrophic problem.
- I don't know why people feel the tool can not be justified unless they find a problem with it.
- Most technicians look for the "Drama" of networking Baselining and become discouraged when the "Drama" is non existent.
- The fact that you can prove everything is quiet and working well makes the tool useful, not useless.
- Think about:
  - ✓ Your warning lights in your car. Do you become upset if a warning light comes on or stays off?
  - ✓ A Doctors stethoscope. Does the Doctor get frustrated that he hasn't found a problem with your heart?

Urban Legends And Myths.

- In today's network, the information and methodology of most technicians are passed down from the past 10 years of knowledge. Unfortunately today's networks don't resemble to what was supported 10 years ago. Hopefully….
- These attitudes and rules of thumb in many cases, are very dangerous and inhibit your ability to properly design, troubleshoot or document a network.
- How comfortable would you feel if you find you found out that your doctor or mechanic has not had any training in the past 10 years.
- How comfortable would you feel knowing that this same person works from '**old wives tales' and legend**, rather than fact?

1. 'If It Ain't Broke Don't Fix It'…

- In the 'old' days, things ***broke and failed***. Unfortunately today things rarely ***break and fail.*** Today things typically ***break, recover and eventually slow down***.
- Your network devices will report problems every day, 7/24. Many of these errors are normal and some are required to make your applications 'work'.
- Many network problems are a result of an accumulation of many small problems or misconfigurations that finally cause the infrastructure to collapse.
- When you believe a '*problem*' is finally resolved, without identifying the true root cause, the '*problem*' invariably returns and labeled as a different problem. Go ahead, ask people if they've ever thought they 'fixed' a problem, only to mysteriously have it return at a later date.
- My point here is, '*not **one** 'thing' breaks anymore, many things are misconfigured*'.

So how do you determine what is misconfigured and how to fix it?

How do we know what a 'good' or normal error is?

What is 'normal', where's that baseline?

Errors What Errors?

Here's an assignment:

- What are your most common types of errors?
  - ✓ Ethernet -
  - ✓ Token Ring –
  - ✓ Cabling –
  - ✓ How does a Full/Half Duplex mismatch look via error counters?
  - ✓ ICMP errors?
  - ✓ Microsoft "Station not in Domain Computer"
  - ✓ TCP Frozen Windows
  - ✓ TCP Zero Windows
- Better question how would you find out?
  - ✓ Via SNMP from your switch?
  - ✓ Span or mirror your port to a Protocol Analyzer?
  - ✓ Span or mirror your port to other types of testers (Cable, RMON probe)?

2. More Bandwidth or Processing Power.

- In today's LANs there is more than enough bandwidth for the average client. I typically ask two important questions to illustrate this point;
  - ✓ How much bandwidth does your top 5 apps require?
  - ✓ What is the maximum bandwidth your PC's take advantage of during a file transfer to/from your local server?
- If your answer starts off with, '***it should be'*** or '***I think***..' then you ***DON'T KNOW***. So find out!
- In an industry of specifics, we don't need more opinions.
  - ✓ **WE NEED MORE FACTS!!**
- In many instances, more bandwidth results in less throughput.

Bandwidth Homework

Here's the scenario:

- I would like you to go back to your desk and copy a 12 MB file (if you're on 10 Mb Ethernet) or 120 MB (if you're on 100 Mb Ethernet) to one of your servers.
- The server should be the one you login into to, or has the most drives mapped to your PC.

Here's the assignment; what kind of throughput did you get **writing** to your server of choice?

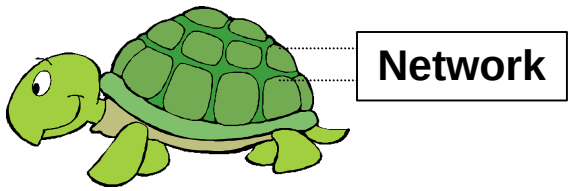
- Better question how would you measure this?
  - ✓ Using SNMP from your switch port?
  - ✓ Span or mirror your port to a Protocol Analyzer?
  - ✓ Span or mirror your port to other types of testers (One Touch)?
  - ✓ Download a utility off the web like AnalogX's Netstat Live(www.analogx.com)?
  - ✓ Use Microsoft's Perfmon (if available)?

Here's the next assignment; what kind of throughput did you get with a **read**?

- If you're on a 100 Mb connection, try 10 Mb to see what kind of gain you may get.
- If your full duplex, try half duplex or vice versa.

3. The 'Slowdowns' Are Always Network Related.

- I'm surprised how many times I hear, ***'it's the network again'*** from technicians who have just approached a problem. These are the same clairvoyant folks who never knew the details of the symptom or resolution, but insist all their woes are a direct result of '**network problems'**.
- Did you know a big box in your corporation labeled, '***THE NETWORK***' does **NOT** exist?
- I think this concept evolved from the mainframe days when a 3174 controller or a FEP health impact hundreds, if not thousands of mindless terminals. Networks today are comprised of many cables, hubs/switches, routers, firewalls, etc…
- If ***'things are slow'***, we should start our investigation by defining the words **'things'** and **'slow'**.



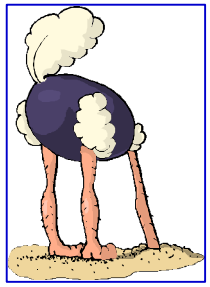
Reasons Why Things May Be Slow.

- Here's several common reasons why things may slow down:
  - ✓ Broadcast storm.
  - ✓ Half/Full Duplex mismatch
  - ✓ Overloaded Application
  - ✓ Inefficient SMB/CIFS Read Write Sizes
  - ✓ Zero TCP Window Sizes
  - ✓ Inefficient applications
  - ✓ Cabling issues Interference
  - ✓ UDP Broadcast forwarding gone awry
  - ✓ Improper frame sizes
  - ✓ Overloaded Server
  - ✓ Overloaded Workstation

- How do you determine if you have the above issues?
  - ✓ Protocol Analyzer
  - ✓ RMON Probe
  - ✓ Cable Tester
  - ✓ Microsoft SMS, Insight Mananger

4. We Don't Have Any Problems?

- Errors on a network are normal, much like hearing the traffic report and learning that there is an accident on a major highway. Some errors such as ones reported by ICMP and topology errors are to be expected. Many of these errors are always occurring, but the network devices involved recover and life goes on.
- This mentality is another 10 year old one where the only problems were 'outages'. Basically these people are waiting for problems to ***'come to them'***. Unfortunately these outage scenarios are rare and are usually the result of something obvious like a change gone awry.
- Problems today revolve around 'slow downs', 'connectivity' and those "X File" type problems that came and went without a real solution.
- Well in the network world, these unexplained phenomenon are typically categorized as ***'hiccups"*** or ***'blips'*** and quickly dismissed.



Common Baselines

- Baselining is often a forgotten art and most people don't baseline for the following reasons:
  - ✓ When should I start?
  - ✓ What should a baseline look like?
  - ✓ What if someone actually reads it and wants more information?
  - ✓ Why bother? Everything changes so fast around here.
  - ✓ I don't know how to baseline.
- Baselines should be:
  - ✓ Clearly defined. For example Bootup baseline, Login baseline, Application Baseline or Upgrade Baseline.
- As long as your goal is clear and the methodology is documented your baseline is correct.
- If you have performed a baseline correctly, you will typically find problems to fix along the way.

5. We Don't Have Time to Learn Another Tool?

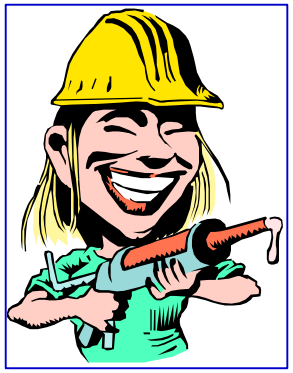
- In the technology world, this statement doesn't sit well with me and is totally unbelievable.
- We make time to re-learn for every Microsoft upgrade, a new PC product or when installing some new network equipment.
- It actually takes more effort and costs more in the long run to ***'not learn'*** and to ***'shoot in the dark'***, than a ***'structured informed approach'***.
- Tools that are vendor independent provide the quickest payoff.
  - ✓ A protocol analyzer will reveal what is going on at the wire level regardless of vendor.
  - ✓ A cable tester will identify cabling issues regardless of vendor, etc..
  - ✓ SNMP RMON consoles will report from any SNMP/RMON enabled device.
- Since these tools work with various vendor's equipment, you typically train less.
- Vendor specific tools would compliment these core set of tools.

Type of Tools

Type of Tool	Are You Responsible	If so, What is your tool, or tools of choice?
Cable Testing		
SNMP/RMON		
Protocol Analysis		
Application Port Monitoring		
Bandwidth Shaping		
Red Light Green Light		
Reporting Tools		
Server Monitoring		
Equipment Element Manager		

6. We Can Do Everything With Our Existing **Tool**.

- The interesting part of this answer lies in the singular use of the word '**tool'**.
- In today's world, verifying that a connection ***'works'*** is not typically an issue. How many times is that link light **NOT** on? Documenting why the connection is ***'slow'*** is far more realistic.
- Gathering information and baselining is a goal, but with many different protocols, applications and various vendors, reality makes this goal seem a dream. No one general purpose tool can ***'do an all encompassing baseline'***.



7. This Tool Is Too Expensive $$$

- This argument makes me wonder what this person does for a living.
- A 1,000 node switched environment will easily cost $100,000 to implement and another $50,000 to install a management system. Don't forget the salary ($40,000) for the staff of approximately 5 to maintain the equipment. About another $5,000 a year for each staff to stay current on the technology.
- Not to mention the obvious fact that the company's core day to day operations depend on data to flow through this network.
- The network management and switch training is vendor specific, which makes me wonder how unbiased this same group will be when evaluating competing technologies after this equipment is deployed. It also becomes difficult to troubleshoot problems with a staff all trained with the same methodology.
- In these environments' I find it amazing that these same people would question a truly independent tool that can identify how well the combination of devices that make up a true network infrastructure is behaving. And more importantly, how well any device behaves on the wire.

8. Broadcast Storms… The Truth!

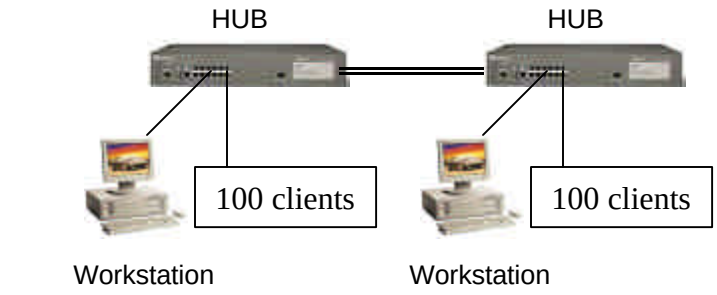
- Many technologists believe that by installing more bandwidth and collapsing network architectures', the threat of a broadcast storm disappears.
- When several segments are collapsed into one large one, the chance of a broadcast storm increases.
- In summary, when you collapse many separate segments into one large one, the workstations/servers will have to process more broadcast packets. So how do you identify and minimize the source of your broadcast packets?
- You should plug a protocol aware tool into any switch port configured for a customer VLAN and observe the protocols in use. NO spanning or mirroring is necessary.

Broadcast Storms - Homework

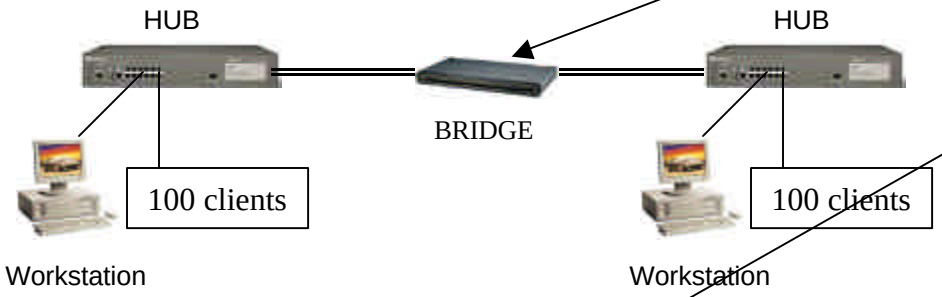
Protocols Available	Protocols You Need	Protocols You Have
IP – Ethernet II		
IP – SNAP		
IP – SAP		
IPX – RAW		
IPX – SAP		
IPX – SNAP		
IPX – Ethernet II		
NetBeui		
Appletalk		
Others		

ARE WE THERE YET ??

Are you going around an implementation merry-go-round blindfolded, controlled by confusion and a lack of network information?

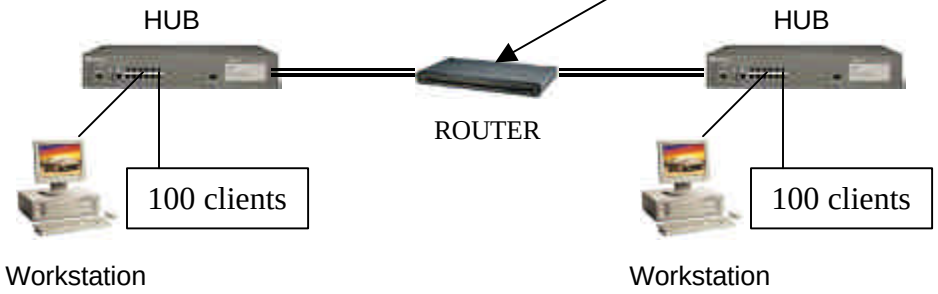


- 200 node Layer 2 Broadcast domain
- 200 Node Collision domain
- Physical level errors propagated
- **IMPLEMENT A BRIDGE TO SEGMENT AT LAYER 2**



- 100 node collision domain
- 200 node Layer 2 Broadcast domain
- Too many broadcasts

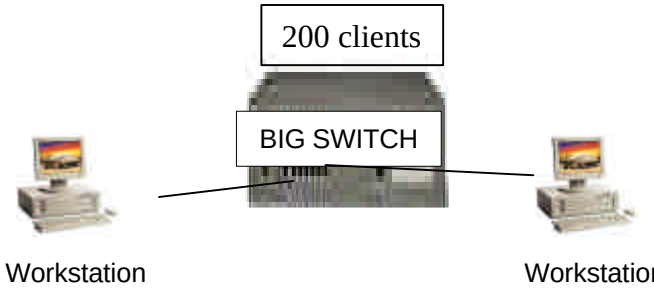
IMPLEMENT A ROUTER TO SEGMENT AT LAYER 3



- 100 node collision domain
- 100 node Layer 2 Broadcast domain
- Routing is slower than switching

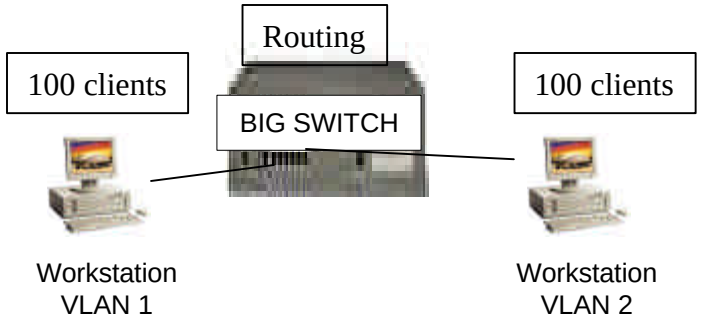
Implement One Huge Switch

And The Reason For All This Is…..?



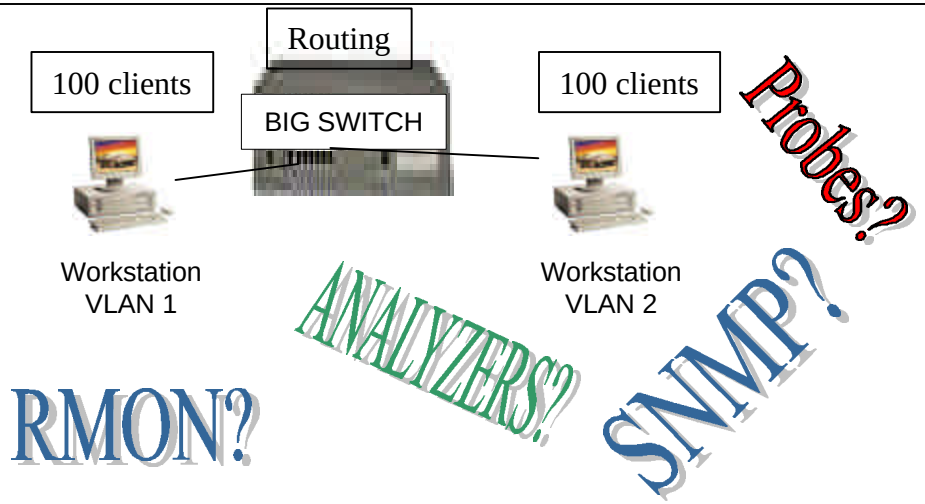
- 1 node collision domain
- 200 node Layer 2 Broadcast domain
- Too many broadcasts

IMPLEMENT VLANS



- 1 node collision domain
- 100 node Layer 2 Broadcast domain
- Still too SLOW

Implement Reporting Tools



- Buy a Lot of Rmon probes and a reporting console.
- Enable SNMP/Rmon on all Supported Devices.
- Install Reporting Software with Database backends.
- Ignore all the data.
- Attempt to decipher the data during an outage.

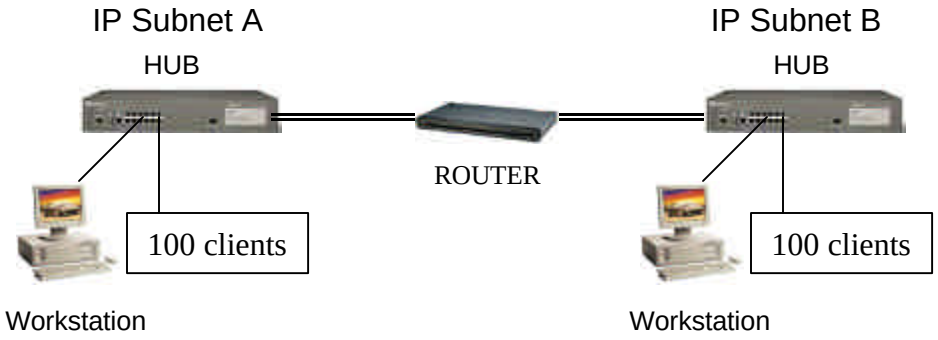
Layer 2 And VLANS

- All troubleshooting, implementation and design activity should begin at Layer 1.
- At layer 2 we have bridging or switching.
- In some cases, the VLAN or broadcast domain may have gotten too large.
  - ✓ How many devices does it take before it is considered ‘large’?
  - ✓ How do we find out how many devices are currently and actively in this VLAN configuration?
- You should also use the same tool you used for the protocol exercise and discover the number of network devices in each VLAN.
- Why have you implemented VLANS?
  - ✓ To reduce congestion? Switching was supposed to fix that.
- I many cases you probably started by segmenting your hubs into smaller groups and connected them to various router ports. This was supposed to relieve excessive congestion.
- Then you removed the routing since it is slower than switching.
- But now you have a large broadcast domain again… Hmm sound familiar?

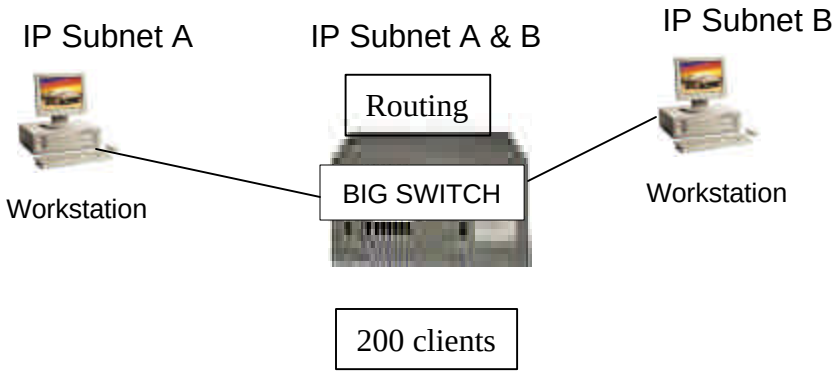
More Design Dilemmas

- Existing network design:
  - ✓ Multiple router interfaces with multiple switches or hubs.
- Goal to reduce costs and leverage the speed of switching over routing.
- But will you achieve it?

Before



After



How did we make out?

What To Ask Yourself ?

- Who can identify your company's most critical applications?
- Have you implemented/upgraded network equipment, servers or applications and **wondered** if your performance got better? What was the goal of the upgrade?
- After completing your implementation/upgrades has performance done down?

So how do you 'really' know if the upgrade 'fixed' or 'broke' anything?

- We all have experienced the placebo effect where we believe there is a performance increase. Over time though we notice things aren't really that much better and the color change or barometric pressure drop really didn't do too much.

Tools are used to gather data and prove or disprove a solution was effective.

More Questions To Ask Yourself.

- Do you experience reoccurring ‘Network Brownouts’ or ‘Slowdowns’ and can’t find the real root cause?
- Does it take a long time to login to your ‘network’ in the morning, or how long does it take to login in the morning?
- Does it take a long time to launch an application, or how long does it take to launch that one application?
- How many application induced coffee/smoke breaks do you know of?
- Does geographic location, day or the week or client configuration affect your response time?

Is Your Network Built for Connectivity, Performance or Convenience?

- Believe it or not, your network design was originally chosen with a specific purpose in mind.
- For example, were you to provide connectivity, security or stability.
- As your network evolves, technology changes and your staff moves on, the original intent of the network will also change, **but who has clearly stated the new goal of the network.**
- Better question, **"who is validating that the new design is indeed meeting these goals."**
- A perfect example is the introduction 802.11b wireless technology.
- Think about it; how many people in your office have laptops that stay bolted to their desks via keyboards, mice, docking stations and 18" monitors? How many people in your company typically bring a laptop in a meeting to take minutes, etc?
- So now people who installed wireless technology without a clear a concise goal for their networks are the same ones complaining about performance and security. And still people are purchasing hubs, etc…

What About My Phone??

- Another network trend we've been seeing is convergence with Voice and Data.
- This started back in the ISDN days, then resurfaced with the ATM days and now we see it again with the QOS days.
- How many of you have sorted how all the "tribal issues" that voice convergence will bring to your firm?
- How do you think the Voice people feel plugging their phones into a shared network where they hear about all the nonsense from security issues to peer to peer software chewing up bandwidth?
- What I've seen in the past would give you whiplash with the amount of money spent to turn a Data network into a Voice network.
- When VOIP is finally installed, the tribal issues rear their ugly head.

You should always plan in advance with all stakeholders and decide how the application will be supported, what are the application requirements, how will your verify the existing application metrics and how will you monitor the application metrics moving forward.

What Is The **Network** In "**Network Management**"?

Network Management is defined as: *(www.webopedia.com)*

- Refers to the **broad subject** of managing computer **networks**. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:
  - ✓ **Security**: Ensuring that the network is protected from unauthorized users.
  - ✓ **Performance**: Eliminating bottlenecks in the network.
  - ✓ **Reliability**: Making sure the network is available to users and responding to hardware and software malfunctions.
- Define your **network** components or audit your mission critical **applications**
  - ✓ Start from a client, their application and the server.
  - ✓ Every component between the client and the server, should be identified and have a clearly defined support process in place.
  - ✓ An Application Baseline should reveal client protocol dependencies and servers required to make the application work.
- Every component must have the following areas identified:
  - ✓ **Fault management**
  - ✓ **Configuration/Security management**
  - ✓ **Performance management**.

What Are You Looking For?

- In the old days people bought network discovery tools to find out if users put a new workstation out there.
- Then the same tool was resurrected to search for rogue hubs or network devices that the user community may have installed.
- Now people are using reporting tools to figure out what applications and how much data their users require.
- We even see people buying software to find out if their users are installing unauthorized software, switches or Wireless Access points.
- Clients should understand their role as a client and the IS division's role.

Where Do You Start?

- When you baseline or troubleshoot where do you start?
- It is quite common for a help desk person to ping a server with the application that a client may be complaining about.
- Is a ping the same as running the application?
- Do you dismiss the issue as a local issue since no one else has complained … **YET!!!**
- Do you start troubleshooting near the server, on the Gig backbone, or near the client?
- I typically approach problems and baselines from the clients' perspective.

Tony's Top Ten Customer Issues. (sort of)

1. Client Misconfiguration – Protocol Bindings
2. Client Misconfiguration – Ethernet Auto Negotiation
3. Client Misconfiguration – Cabling
4. Client Misconfiguration – Unnecessary Services

5. Server Misconfiguration – Protocol Bindings
6. Server Misconfiguration – Ethernet Auto Negotiation
7. Server Misconfiguration – Cabling

8. Network Device Misconfiguration – Full Duplex/Half Duplex
9. Network Device Misconfiguration – IP/Broadcast Issues
10. Network Device Misconfiguration – Spanning Tree

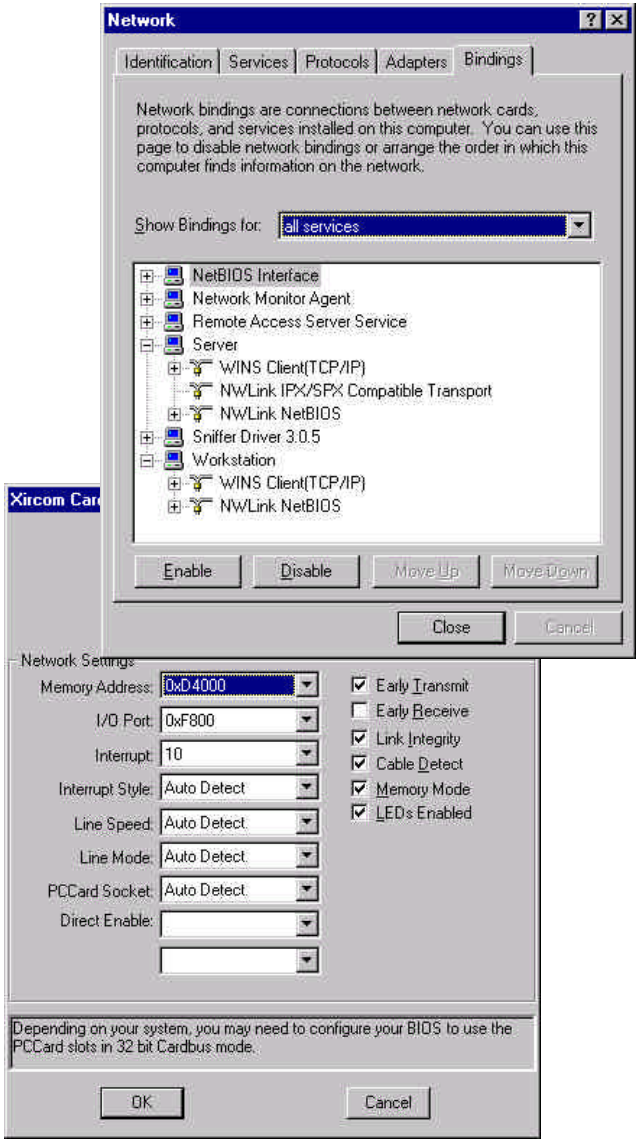
11. Application Issues
12. Latency and Throughput Issues
13. **No Documentation of any kind**

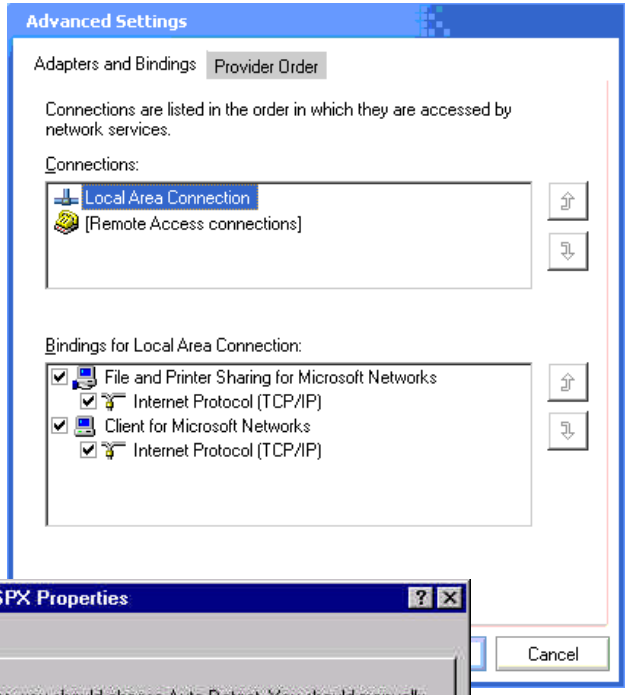
Client & Server Misconfigurations

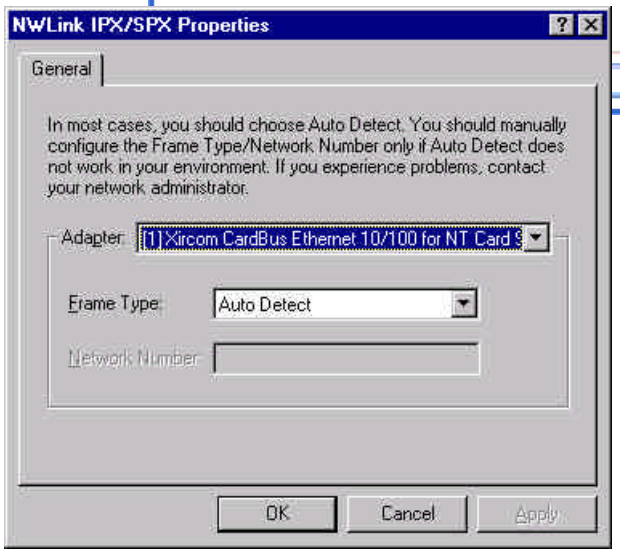
- In the past few years the Networking industry has gone from ***precise planning and understanding*** to leaving most of the networking parameters to '*plug and pray*'.
- In our defense, most of today technologists are too busy to stop and investigate every little setting available and their impact.
- I call this the new networking sitcom, '**Everybody Loves Auto'**. The title pretty well sums it up.
- The **worst** case scenario; *these settings are left alone and hopefully everything 'works'*…. 'Well'…
- The **best** case scenario, *these settings are left alone and you have intermittent stability issues that you do not know how to address.*
- Part of the problem is that our network and nodes are very resilient, most of the time. A day one problem may be covered up only to return as a network issue that is not obvious.

You should attempt to baseline your 'standard' PC/Server builds.

What Client Misconfigurations?







Network Device Misconfigurations

- The same '*auto*' issue exists when technologists install network equipment. In many cases the vendor has enabled many 'features' that eliminate many of the '*simple*' calls they otherwise receive.
- Unfortunately many of these auto settings also cause 'new' problems.
- The majority of the time, technologists don't fully understand the impact that one little 'setting' will have on his network.

What Network Device Misconfiguration

CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port 3/4

msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel misconfiguration of %s %s")

Switch#**debug etherchnl** PAgP Shim/FEC debugging is on
22:46:30:FEC:returning agport Po15 for port (Fa2/1)
22:46:31:FEC:returning agport Po15 for port (Fa4/14)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
22:46:33:FEC:port_attrib:Fa2/25 Fa2/15 same
22:46:33:FEC:EC - attrib incompatable for Fa2/25; duplex of Fa2/25 is half, Fa2/15 is full
22:46:33:FEC:pagp_switch_choose_unique:Fa2/25, port Fa2/15 in agport Po3 is incompatable
Switch#

Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 10.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec

Ethernet 0 is protocol is up
Hardware is Ethernet, addr
0000.0c00.750
0000.0c00.750
Internet addr
1 0.1 08.28.8, subnet mask is 255.255.255.0

Sample Web Browsing Exercise

Web Browsing

- Tony is on the 4th Floor in ACME, Toronto, Ontario.
- The Web server is in the Calgary Data Center.

Lets follow the path from the client to the server.

- Tony is using a Sony laptop with the Windows 98 operating system.
- The laptop is connected to a wall jack via a copper cable.
- The wall jack is wired to the 4th floor wiring room to a distribution rack.
- The cabling terminates at a floor Layer 2 switch.
- The floor switch is connected to a set of core switches via fibre.
- The core switches are connected a router with a frame relay circuit to Calgary via copper cabling.
- In Calgary circuit is also terminated on a router.
- The router is connected, via copper to a core switch.
- The core switch is connected, via fibre to the webserver.

The Lay Of The Land

Client
Tony

Patch
Cable

Face
Plate

Cabling

Patch
Panel

Floor
Switch

Fibre
To
Core

Core
Switch

Direction of the command

Cabling
To Router

Router

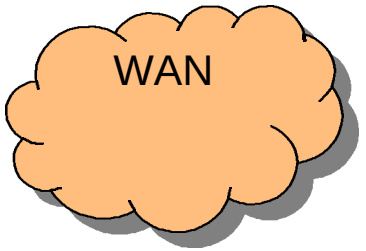
Webserver

Fibre
To
Server

Core
Switch

Cabling
To Switch

Router



Client

- What is so complicated about a client?
  - ✓ Fault management
    - How to handle a simple PC Support Problem?
    - How to determine if the problem is hardware, software or user account?
  - ✓ Configuration management
    - How to validate that the PC is configured appropriately?
    - How and when are Service Packs applied?
    - Are there any unauthorized applications installed?
    - How are user id's created and assigned?
    - Are ID's and passwords changed on a regular basis?
    - Is Dynamic DNS causing any issues?
    - Is encryption required for internal applications?
  - ✓ Performance management
    - How to handle slow response?
    - What is the typical response time or throughput to your application server?
    - How do you test performance?
- What is available?
  - ✓ Compaq's Insight Manager, Dell's IT Assistant, Intel's LANDesk
  - ✓ Protocol Analyzers
  - ✓ SNMP/RMON
  - ✓ Ping
  - ✓ Manual inspection

Cabling




- What can possibly go wrong with a wire?
  - ✓ Fault management
    - How to handle a simple cable break?
    - How to determine if the problem is the wire, connector, etc?
    - How to maintain your fiber connections?
  - ✓ Configuration management
    - How to validate that the cable is within specification?
    - Are there any non standard cables installed?
    - Are any cables near a source of electromagnetic interference?
    - Can anyone buy a cable and just plug it in?
  - ✓ Performance management
    - How to determine if cabling does not meet spec?
    - Can you run 100 Mb, 1 Gb or 10 Gb over your existing cabling?
- What is available?
  - ✓ Cable testers
  - ✓ Cabling companies
  - ✓ SNMP/RMON
  - ✓ Manual inspection

Switch

- What can possibly go wrong with a switch after installation?
  - ✓ Fault management
    - Is auto negotiation working?
    - Are there excessive errors?
  - ✓ Configuration management
    - Is spanning tree configured properly?
    - Are other proprietary commands used?
    - What policy is used when creating VLANS?
    - Is backpressure or pause frames in use for flow control?
    - What devices are connected to which ports?
  - ✓ Performance management
    - How you decide the speed and duplex mode for your ports?
    - Is SNMP/RMON enabled?
- What is available?
  - ✓ SNMP/RMON consoles
  - ✓ Manual review of stats
  - ✓ Protocol Analyzers
  - ✓ Specialty cable testers

Routers

- Don't routers just route?
  - ✓ Fault management
    - How to detect if a router is still routing?
    - How and how often to check if an interface is down?
    - How to check if the proper protocols are enabled?
  - ✓ Configuration management
    - Who determines filtering policies?
    - Who creates id's for the technicians?
    - How are routing policies set?
    - When are maintenance windows?
  - ✓ Performance management
    - Is the router dropping packets?
    - Is SNMP/RMON enabled?
- What is available?
  - ✓ SNMP/RMON consoles
  - ✓ Manual review of stats
  - ✓ Protocol Analyzer

Server

- Don't we just configure a server and leave it in "auto pilot"?
  - ✓ Fault management
    - How to determine if the problem is hardware, software or user account?
    - Logistics involved in restoring data backups or server replacements.
  - ✓ Configuration management
    - How to validate that the server is configured appropriately?
    - Are there any unauthorized applications or backdoors installed?
    - How are supervisor id's created and managed?
    - Are ID's and passwords changed on a regular basis?
    - How are changes managed and reviewed?
  - ✓ Performance management
    - How to handle slow response?
    - What is the typical response time or throughput to your application server?
    - How do you test performance?
- What is available?
  - ✓ Compaq's Insight Manager, Dell's IT Assistant, Intel's LANDesk, Microsoft's SMS
  - ✓ Protocol Analyzers
  - ✓ SNMP/RMON
  - ✓ Ping
  - ✓ Manual inspection

And Of Course, The Application

- If you thought that the application was the least of your worries, you've got a rude awakening on its way.
- The Application may be obvious, for example;
  - ✓ An email application
  - ✓ a web browser of choice
- The application may be a lot less obvious, for example;
  - ✓ Microsoft Client
  - ✓ Novell's Netware client
  - ✓ NETBios
  - ✓ VPN client
- So what?! If I click the icon and I don't see an error message, then everything is OK.
- The issues today revolve around performance, so we have to dissect the way in which the application behaves.
- Some typical Application issues;
  - ✓ Frame Size
  - ✓ Excessive broadcasts
  - ✓ Unknown server dependencies
  - ✓ Version differences

Miscellaneous Notes

- You may have other network components (physical or software) that introduce added complexities. These devices and software need to be taken into consideration when we plan, implement or attempt to support these devices.
- For example,
  - ✓ If bandwidth shaping is used, where is the shaping performed? Is it software on the client's PC, an external physical device, or is it accomplished with your routers?
  - ✓ Firewalls are typically present in most corporate environments. Since a firewall is transparent in nature, how to verify if its up, is someone monopolizing the bandwidth, are packets being dropped?
  - ✓ DHCP is prevalent for obvious reasons. How many DHCP servers do you have? How do you propagate DHCP requests across router interfaces?
  - ✓ DNS servers must be operational for most name resolutions to work. How many re in your environment and how do you check its up time.
  - ✓ Service Level Reporting is becoming a necessity. Where do you report client response time? Do you just check a device's availability via a ping or port check? Do you simply take the SNMP uptime and report it?

In Summary

Ensure you have the proper :

- Internal understanding of who is responsible for various technology components.
- Policies in place to support you.
- Tool for the proper job.
- Training to understand the data that the tool reports back to you.
- Design goals from your client.
- Plan to verify changes resulted the way you had hoped.
- Methodology to use your existing tools in your environment properly.

Start 'Documenting and Baselining' today, tomorrow is always too late.