

NETS Training

Troubleshooting

Scot Colburn and David Mitchell

5/1/07

What Is Troubleshooting

- The fixing of problems
- Problems reported by users
- Problems detected by monitoring
- Problems you made for yourself

How Is It Done?

- Identify undesirable behavior
- Locate root cause
- Fix the problem
- Finding the root cause is usually most of the battle
- Many problems are easy to fix once the source is identified

What Makes It So Hard?

- Pressure: the clock is ticking
- Unfamiliar territory
- Management Access is Broken
- Counters Sometimes Lie
- Preconceived Notions

Pressure

- Operations is calling
- Users are standing in your office
- Have you sent an outage notice?
- Your outage window is over

Unfamiliar Territory

- Running commands which are not normally used
- Looking at counters which are not normally looked at
 - You can find errors all over the place once you start looking. How many of those are normal?

Management access is broken

- Can't get to the device you need to look at
 - No direct access
 - Perhaps only one at a time via serial or dialup
 - DNS may be unavailable

Sometimes counters lie

- A zero isn't always a zero. It may just mean the value isn't being properly counted.
- Some counters only update periodically, so repeated 'show' commands may show the same value even though it's going up.

Preconceived notions

- Sometimes the real problem is overlooked because of bad assumptions made early on.
- Assuming a historically problematic device is part of a current problem
- Skipping past the simple explanations

How Can We Make It Easier

- Use the OSI Seven Layer Model
- Isolate A Specific Reproducible Problem
- Know Your Commands
- Know Your Other Tools

Use The OSI Model

- Layer 1: Physical
 - Do we have link?
- Layer 2: Data Link
 - Is the port in the correct VLAN?
 - Do we have CAM entries?

Use The OSI Model

- Layer 3: Network AKA IP
 - Does the router have an ARP entry
 - Can the router ping it?
 - Does the router have a route?
- Layer 4: Transport AKA TCP
 - Is DNS working?
 - Is TCP tuned properly for the path?

Isolate A Specific Problem

- Find a specific host or pair of hosts which is having problems
- Look for where in the path things break
- Remember, direction is important!

Know Your Commands

- traceroute / tracert
- ping
- nslookup / dig
- ipconfig / ifconfig
- mtr / winmtr

Know Your Commands

- 'show' commands are generally safe.
- Spend some time exploring them.
 - What does what.
 - What is normal?
- CatOS: show port, show mac, show cam, show module, show log, show logging buffer, show counters, show channel, show cdp neighbor, show inline power
- IOS: show interface, show ip arp, show ip route, show ip ospf, show ip bgp

Know Your Tools

- Port Lists
- Cricket Statistics
- Searches
- Nagios
- Configuration Archive
- Syslog

Demonstration

- Tools
- Common Show Commands

