Taking the "Work" Out of Networking: Strategies for Smarter, Simpler Network Architecture and Administration

Building the Connection Between Government, Business, Education, and Technology

NASA

Jet Propulsion Laboratory
California Institute of Technology

GBET

A CENTRIC Event
Taking the "Work" Out of Networking: Strategies for Smarter, Simpler Network Architecture and Administration

- 10/01/2003, 1:30 PM - 2:30 PM

Speaker:
Claudia De Luna, Technical Manager for Network Development and Engineering, NASA/Jet Propulsion Laboratory.

The smooth performance of your network increasingly defines the ultimate success of your agency's IT initiatives. But a network is a living breathing entity that must be painstakingly managed around the clock—or is it? High performance doesn't have to mean high maintenance if you choose your networking equipment and administration tools wisely. This session will help you tune up your skills and knowledge on the latest advances in network design and management, to keep your agency's data communications running at peak performance, with minimal cost and effort.
Agenda

- Background
- Scope
- Philosophy
- Architecture Overview
- Campus Network
- Components of Network Management
- Lessons Learned
Background

- 1995 – JPL IT Organization and CIO determine that network service is key to the JPL mission and that the current de-centralized environment is not cost effective and cannot provide the required service levels.
- Funding is secured to centralize networking and for the capital investment required to install
  - a new cable plant
  - a star or hub based ethernet network
  - A management system for the new network
- Mission: to provide network service to the JPL user community
- The JPL Network Architecture and philosophy reflect this mission
- The network is a utility
Scope

- The JPL network is comprised of over
  - **16,000 network nodes** (i.e. workstations, servers, printers) and
  - **over 800 network devices** (i.e. switches and routers)
- **140 Building and Structures**
- **3 sites**
  - Main campus
  - 12 Satellites
- The network management systems and network architecture we will discuss today help the JPL Network Team operate this network at 99.995% availability.
- JPLNet 24x7 with a 2 hour restoral commitment to our customers
JPLNet Network Availability

Target Availability

Network Device Count

FY 2000
Month (fiscal)

13647 13716 13781 13821 13962 13912 14036 14125 14204 14353 14452 14562
Network Architecture

- 16,000+ Network Devices
- Structured Cabling
  - 3 Category 5/5e to each work location
  - 6MM to select work locations
  - 6SM/18MM riser
  - 12SM/12MM between buildings
- Fully Switched
  - 10/100Mb/s to each desktop [10Base-T/100Base-TX]
    - Limited only by Network Interface Card (NIC) on system
  - 1000Mb/s for approved systems [1000Base-SX]
- Multi-Gigabit Core
  - 18 Cisco 8540 L2/L3 switches interconnected via GigE
- Deterministic
  - 2 Hops
  - Consistent Edge and Backbone Hardware
JPLNet Gigabit Backbone OAK GROVE / IPC

Mission Net

JPL IS Services Subnet

Industry Partners

NASA Internet

Los Nettos/ISI T3/OC-3

Internet

CalREN-2 Internet Abilene vBNS

Isolation Network

Security Monitors

Calix

b171-core 6509

b230-core 6509

b238-edge

b264-edge

b300-edge

b301-edge

b301-edge2

b600-edge

b079-edge

b125-edge

b126-edge

b156-edge

b168-edge

b169-edge

b171-edge

b171-edge2

b180-edge

b183-edge

b171-border GSR

External Wan 7513

Internal WAN 7513

Gigabit Ethernet / OC-12

Fast Ethernet
Services

- Management & Monitoring
  - 800+ Network Devices monitored via NMS
  - 20,000+ interfaces monitored for Utilization
  - 1000Base-SX and 100Base-TX/FX RMON probes

- External Connectivity
  - OC-12s (622Mb/s) to CalREN-2
  - Fast Ethernet (100Mb/s) to commercial ISP
  - OC-3 NASA Networks (155Mb/s)
    - ~50Mb/s to Production Networks
    - ~100Mb/s to Research Network (NREN)
  - NRENv2/NPN – NASA Prototype Network
Services (Continued)

- Connectivity to hosts and resources within JPL
  - 10/100/1000
- Connectivity to hosts and resources external to JPL
  - Commercial Internet
  - Internet2
  - NASA Networks
    - SIP/PIP/EBNet
- JPLNet Address Space
  - DNS
  - DHCP
- Time Service
- Remote Access
  - Dial-up (56Kb/s, ISDN)
  - Virtual Private Network (VPN)
  - SSL
Inventory

- What components do you care about?
- What components make up your network?
- Where are they?
  - On-site spares
  - In stock
  - In operation
- Naming
- Maintenance
Network Device Monitoring and Status

- SNMP based Network Management System to ask “Are you there?”
  - Make sure the components providing service can be managed
  - Make sure you manage them
  - Try to manage all the components between your service and your customers
  - Understand how long it takes to ask each device if it is there and how it is
- Foundation for asking “How are you”?
  - Are you too busy to handle everything?
  - Has there been a sudden change?
- Monitor the Monitoring Systems
Notification

- When a device “yells for help”, disappears, or there is a noteworthy change in the environment, how does anyone know?
  - Normal Business Hours
  - After Hours
- Who do you tell?
- How do you tell them?
# Day Shift Action on Alarm

<table>
<thead>
<tr>
<th>Action</th>
<th>Time Since Alarm without acknowledgement (Minutes)</th>
<th>Total Time Device Down (Minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email NOC</td>
<td>0</td>
<td>6-9</td>
</tr>
<tr>
<td>Page NOC Personnel and Key Engineering Staff</td>
<td>0</td>
<td>6-9</td>
</tr>
<tr>
<td>Page JPLNet Operations Manager</td>
<td>5</td>
<td>11-14</td>
</tr>
<tr>
<td>Page JPLNet Dev &amp; Eng Manager and IS Operations Manager</td>
<td>15</td>
<td>26-29</td>
</tr>
<tr>
<td>Email NOC (Exhausted Actions)</td>
<td>15</td>
<td>41-44</td>
</tr>
</tbody>
</table>

Note: Time is shortened during day because it is expected that the NOC is staffed and will act immediately on alarms.
# After-Hours Action on Alarm

<table>
<thead>
<tr>
<th>Action</th>
<th>Time Since Alarm without acknowledgement (Minutes)</th>
<th>Total Time Device Down (Minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email NOC</td>
<td>0</td>
<td>6-9</td>
</tr>
<tr>
<td>Page On-Call Person</td>
<td>0</td>
<td>6-9</td>
</tr>
<tr>
<td>Page On-Call Coordinator</td>
<td>0</td>
<td>6-9</td>
</tr>
<tr>
<td>Phone On-Call Person on Cell</td>
<td>5</td>
<td>11-14</td>
</tr>
<tr>
<td>Phone On-Call Person at Home</td>
<td>5</td>
<td>16-19</td>
</tr>
<tr>
<td>Page On-Call Coordinator</td>
<td>5</td>
<td>21-24</td>
</tr>
<tr>
<td>Page JPLNet Operations Manager and IS Operations Manager</td>
<td>15</td>
<td>36-39</td>
</tr>
<tr>
<td>Page JPLNet Dev &amp; Eng Manager</td>
<td>15</td>
<td>51-54</td>
</tr>
</tbody>
</table>
Network Monitoring and Notification System Communication

TCP/4998

Monitoring System -> UTILITY Alarm Logging

Web Based Alarm Log

Building A

TCP/4998

Network Monitoring -> Notifications

Notification Software

Paging Line Out
Dialogic Line In

SNPP via Network
TCP/7777

Building B

UDP/161
UDP/162

Monitoring System
Proprietary Heartbeat

Paging Line Out
Dialogic Line In

Net-mon-001

Net-mon-002

Proprietary Heartbeat

Watchdog

TCP/4999

Utility Server
Web Operator
Sun 220R utility

TCP/80
TCP/8080

TCP/7777

SNPP via Network

Building A

TCP/7777

Utility Server
Web Operator
Sun 220R utility

TCP/80
TCP/8080
Capacity Planning

- When will what I have not be enough?
  - When will the tub overflow?
Performance and Utilization

- How much is currently being used?
- Is it working well?
Device Mapping

- Where is this device?
- System to Location
  - Oracle/Scanners
- Connection to User
- System (IP Address) to Switch Port Mapping
  - JPL uses an in-house developed set of tools that help us track a host real-time. This is necessary to track a host real-time since users may move hosts without telling us. This information is used to physically track a port, to check for port/NIC issues such as auto-negotiation problems, and to look at Concord Nethealth reports. Concord tracks each port by the switch name and port number so this mapping is essential if you need to look at any report for that host/port.
  - The findport utility does a real-time arp table refresh and query from the router arp table and then searches through the switches on the subnet for the MAC address.
# Nettools

Example of Nettools findport utility:

## findport jplnetflow

Searching for jplnetflow IP:137.78.167.100  MAC:0800.209E.A31B

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Type</th>
<th>Port</th>
<th>BrTbl</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>b171-b-78-167-13</td>
<td>WS-C4003</td>
<td>Port2/2</td>
<td>1/1</td>
<td>1000</td>
<td>full</td>
</tr>
</tbody>
</table>

## findport rawlins

Searching for rawlins IP:137.78.171.202  MAC:0800.2073.F07F

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Type</th>
<th>Port</th>
<th>BrTbl</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>b171-2-78-171-6</td>
<td>WS-C6509</td>
<td>Port9/36</td>
<td>1/1</td>
<td>a-10</td>
<td>a-half</td>
</tr>
</tbody>
</table>

## findport utility

Searching for utility IP:137.78.167.108  MAC:0800.20C8.8008

<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Type</th>
<th>Port</th>
<th>BrTbl</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>b171-b-78-167-13</td>
<td>WS-C4003</td>
<td>Port2/4</td>
<td>1/1</td>
<td>a-100</td>
<td>a-full</td>
</tr>
</tbody>
</table>
IP Address Management

- Manage your address space!
Cable Management

- Cost
- Commitment
- Invaluable
Ticketing System

• Service Request
  • Request from users which do not involve network outages
  • Configuration Management
    • Requests to ourselves
• Problem Report Tracking
Configuration Management

- Keeping Inventory current
  - Must have a list of operational components or how do you manage them
    - Component fails
    - Component is added or removed
    - Component is upgraded
- What changed, who changed it, and how
What changed and how?

b171-rtr: Comparing version 116 with version 115

< ! Last configuration change at 20:39:44 PDT Fri Apr 19 2002
> ! Last configuration change at 15:23:01 PDT Mon Apr 22 2002
< ! NVRAM config last updated at 20:39:47 PDT Fri Apr 19 2002
> ! NVRAM config last updated at 15:23:23 PDT Mon Apr 22 2002
+ access-list 103 permit tcp host 137.78.169.48 eq smtp any gt 1023
  + access-list 103 deny ip host 137.78.169.48 any
  + access-list 105 permit tcp any gt 1023 host 137.78.169.48 eq smtp
  + access-list 105 deny ip any host 137.78.169.48

b300-edge: Comparing version 28 with version 27

< ! Last configuration change at 13:44:48 PST Thu Mar 14 2002
> ! Last configuration change at 07:51:46 PDT Mon Apr 22 2002
< ! NVRAM config last updated at 13:44:56 PST Thu Mar 14 2002
> ! NVRAM config last updated at 07:51:54 PDT Mon Apr 22 2002
- ip helper-address 137.78.7.50

SUMMARY

Successful b171-rtr
Successful b300-edge

Started: Tue Apr 23 01:42:00 PDT 2002
Ended : Tue Apr 23 01:42:08 PDT 2002
IDS (New)

- Monitoring Additional Duty
- Focus on Network based Intrusion Detection Systems
- Correlation and Integration with Management Systems
Baseline Performance

- ...of your network and your network monitoring systems
- Testing results from generating alarm events using the new LAN container show that longest time to alarm in Spectrum was 1 minute and 52 seconds.
  - If the alarm was sustained for 6 minutes, it would have generated an Attention Notification event.
- The longest time to clear an alarm in Spectrum was 3 minutes and 14 seconds.
Troubleshooting Tips

• Test “Rig”
Staffing

- Operations Staffing
  - NOC Desk 3
  - Operations Field Staff and Support 11
- Development Staffing (10 Development & Sustaining)
  - 1 Sustaining Engineer
  - 1 Capacity Planning/Monitoring
  - 1 Notification/Monitoring/Metrics
  - 1 Database Person (Oracle/Access)
  - .25 Mapping
  - .25 Ticketing System

- 4 Person on-call Rotation
- Highly Cross-Trained
Future

- Application Response Time
- End to End performance
- Correlation
- Security Devices
- Monitoring at 10GigE
- Tools for user testing
- Monitoring Delay and Jitter
Lessons Learned

- Minimize the type of components
- Make sure you can manage your components and that you do
- Keep your list current
- Understand your traffic flows
- Start building the framework that will allow you to instrument for voice and video
- Always fight for simple