NET311
Computer Networks Management

Dr. Mostafa H. Dahshan
Department of Computer Engineering
College of Computer and Information Sciences
King Saud University
mdahshan@ksu.edu.sa

Introduction

- A network consists of many complex, interacting pieces of hardware and software
  - links, switches, routers, hosts
  - other physical components
  - protocols that control and coordinate these devices
- It is not surprising that components will occasionally malfunction
  - network elements misconfigured
  - network resources will be over-utilized
  - network components will simply “break” (e.g. cable cut)

Introduction

- Network administrator’s job is to keep the network “up and running”
- Must be able to respond to (better yet, avoid) such mishaps
- With thousands of network components spread out over a wide area
- Network operations center (NOC) clearly needs tools
- Tools help monitor, manage, and control the network

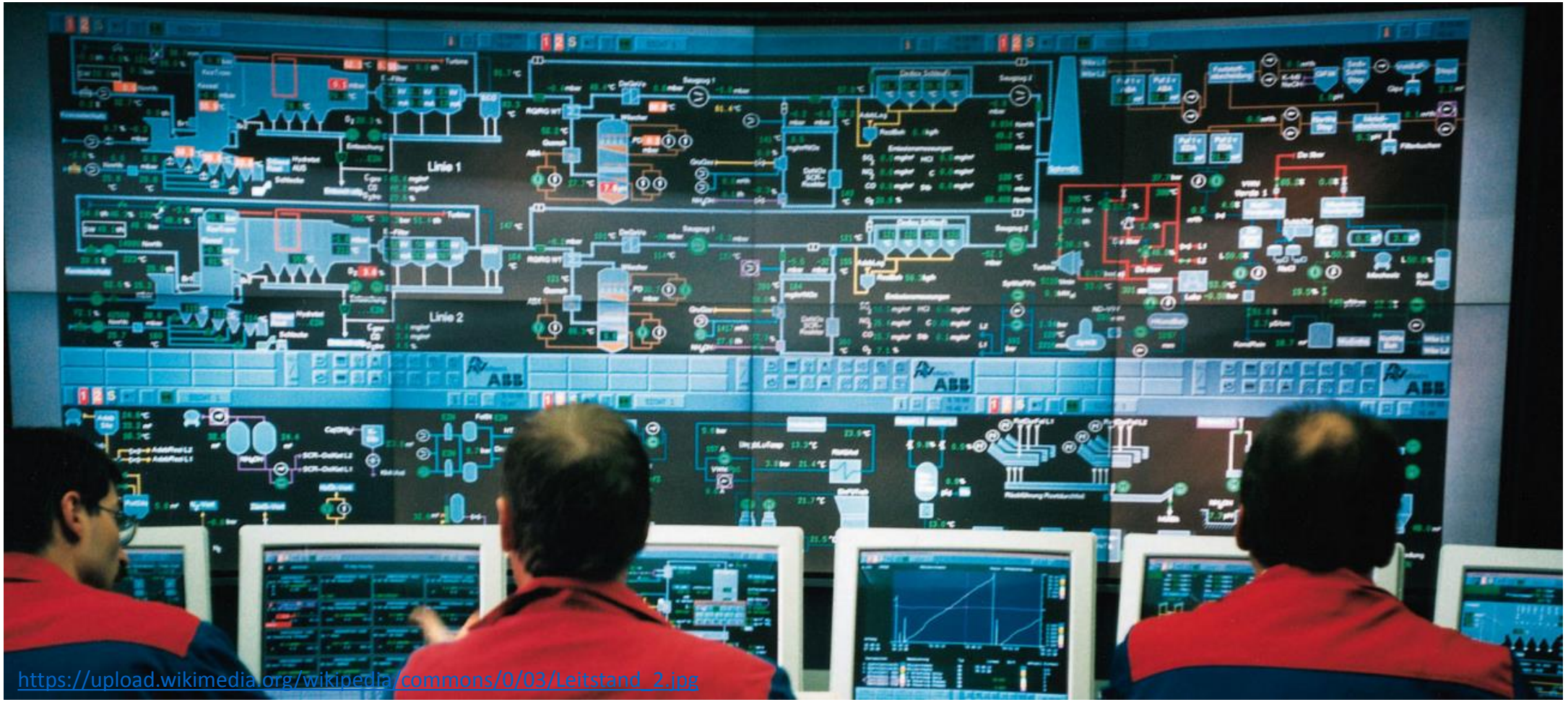
Analogy: Electrical Power Plant

- Electrical power-generation plants have a control room
  - dials, gauges, lights
- monitor the status of
  - remote valves, pipes, vessels (أوعية)
  - and other plant components
- These devices allow operator to monitor plant's many components
  - may alert the operator when trouble is imminent (وشيك)
- Actions are taken by plant operator to control these components

Analogy: Electrical Power Plant

https://upload.wikimedia.org/wikipedia/commons/8/8d/NS_Savannah_control_room_MD1.jpg

Analogy: Electrical Power Plant



https://upload.wikimedia.org/wikipedia/commons/0/03/Leitstand_2.jpg

Analogy: Airplane Cockpit

Instrumented to allow pilot to monitor and control the many components that make up an airplane

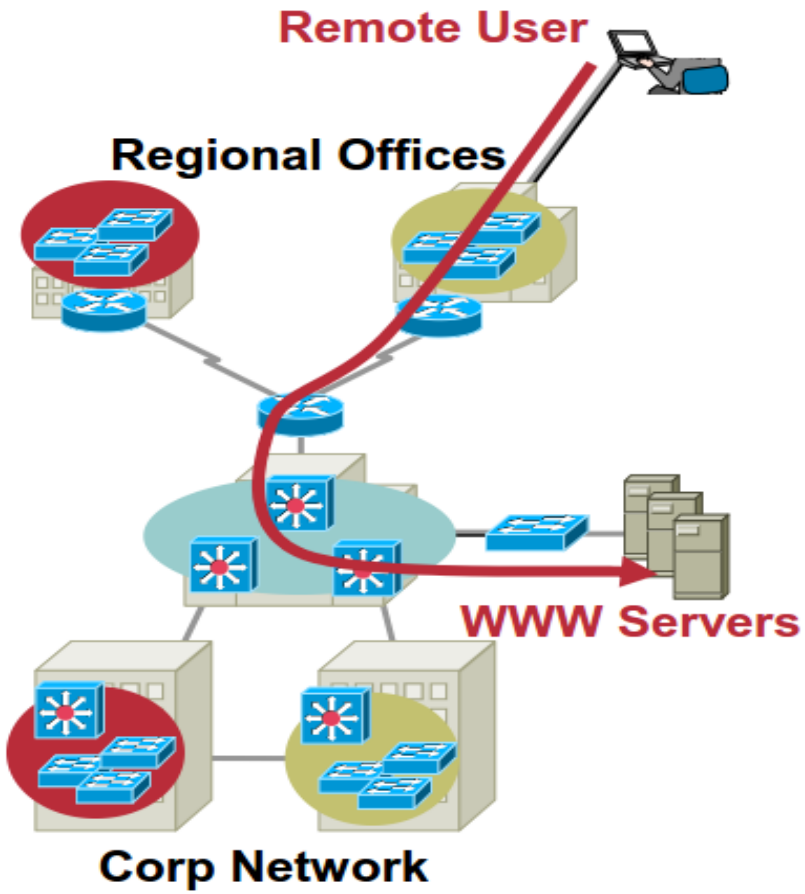
http://www.embraerexecutivejets.com/nva/img/old/jets/legacy/Legacy_Executive_Aircraft_Cockpit.jpg

Analogy

- In these examples, the “administrator”
  - monitors remote devices
  - analyzes their data
  - ensure that they are operational and operating within prescribed limits
  - e.g.,
    - core meltdown of a nuclear power plant is not imminent
    - plane is not about to run out of fuel
  - reactively controls the system by making adjustments in response to changes
  - proactively manages the system
    - detecting trends or anomalous behavior
    - allowing action to be taken before serious problems arise

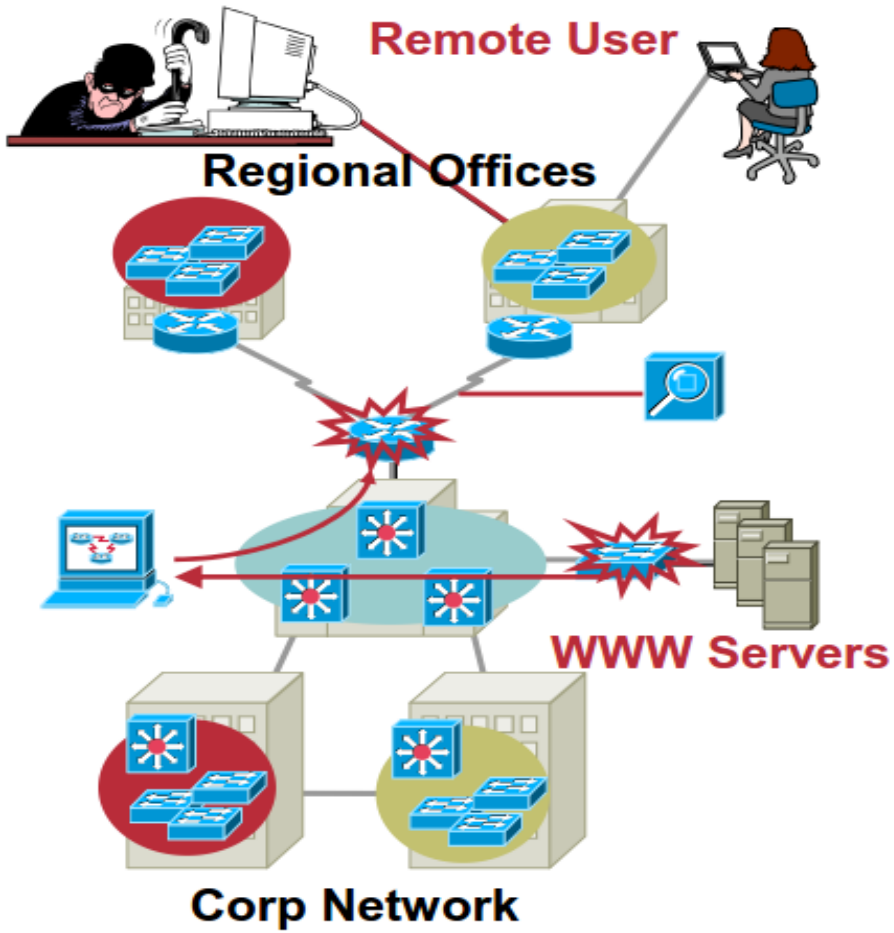
The Case for Management

- **Typical problem**
  - Regional user arrives at work and experiences slow or no response from corporate web server
- **Where do you begin?**
  - Where is the problem?
  - What is the problem?
  - What is the solution?
- **Without proper network management, these questions are difficult to answer**



The Case for Management

- With proper management tools and procedures in place, you may already have the answer
- Consider some possibilities
  1. What configuration changes were made overnight?
  2. Have you received a device fault notification indicating the issue?
  3. Have you detected a security breach?
  4. Has your performance baseline predicted this behavior on an increasingly congested network link?



ROI Example
Using a Management Tool for Daily Tasks

Number of Managed Devices		**800**
Average Manual Process Time Required (Man-Hours)		
Software Upgrade	**0.05**	**(3 Min/Device/Qtr)**
Password Change	**0.25**	**(19 Min/Device/Bi-Annual)**
Gather Inventory Information	**0.03**	**(2 Min/Device/Qtr)**
Documenting Changes	**0.08**	**(5 Min/Incident)**
Audit	**30.00**	**(Per Qtr)**
Cost per Man-Hour $48.84	**Manual Configuration Error Rate 2%**	

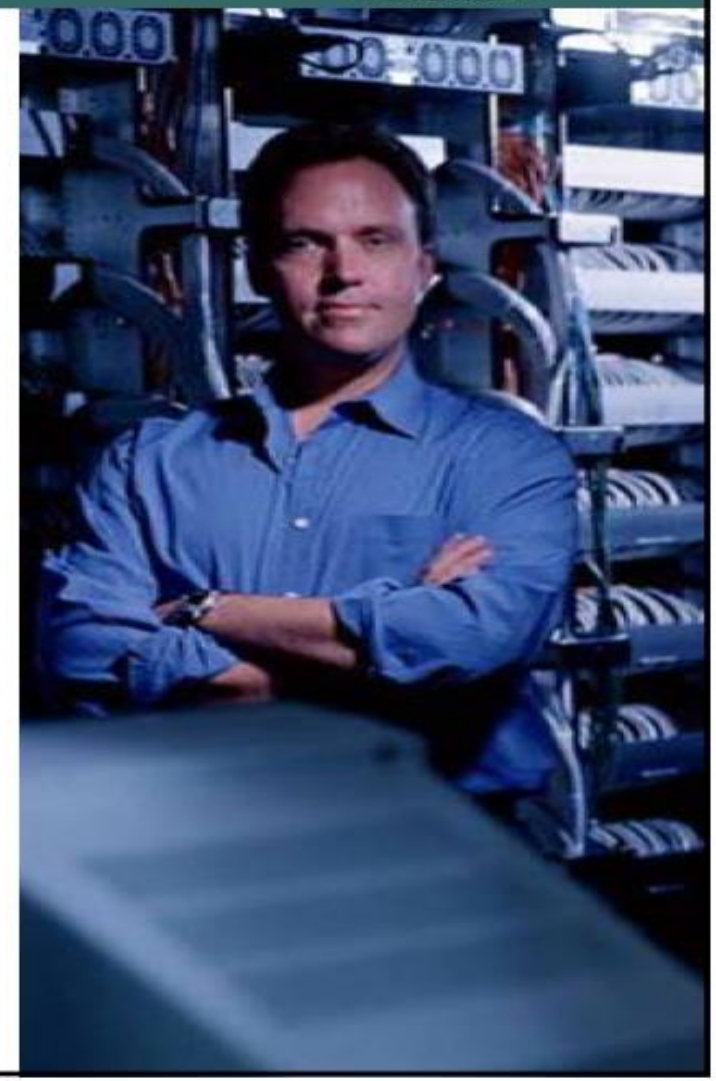
Configuration Management Process	Manual Procedure Required Man-Hours (per Annum)	After Product Implementation Required Man-Hours (per Annum)	Time Savings	ROI
Password Change	**435**	**44**	**391**	**$19,106.21**
Software Upgrade	**544**	**0.37**	**544**	**$26,551.05**
Gather Inventory Information	**381**	**0.67**	**380**	**$18,565.71**
Documenting Changes	**120**	**0.67**	**119**	**$5,828.24**
Total Configuration Management ROI				**$70,051.21**

Source: Cost Analysis Using CiscoWorks LAN Management Solution. Esaka, 2002

The Network Manager's Responsibility

Cisco.com

- Ensure that the users of a network receive the information technology services with the quality of service that they expect
- Strategic and tactical planning of the engineering, operations, and maintenance of a network and network services
- Help network engineers deal with the complexity of a data network and to make sure that data can go across it with maximum efficiency and transparency to the users



What is network management?

- “Network management includes the deployment, integration, and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.” [T. Saydam and T. Magedanz]

Network Management Defined

Network Management

Key Network Management Tasks	Key Network Management Success Factors
Monitoring	Control
Configuration	Productivity
Troubleshooting	Efficiency
Administration	VoIP, VPN, QoS

Simple Scenario

- A small network that consists of
  - three routers
  - some hosts and servers
- Even in such a simple network, admin can benefit from network management tools

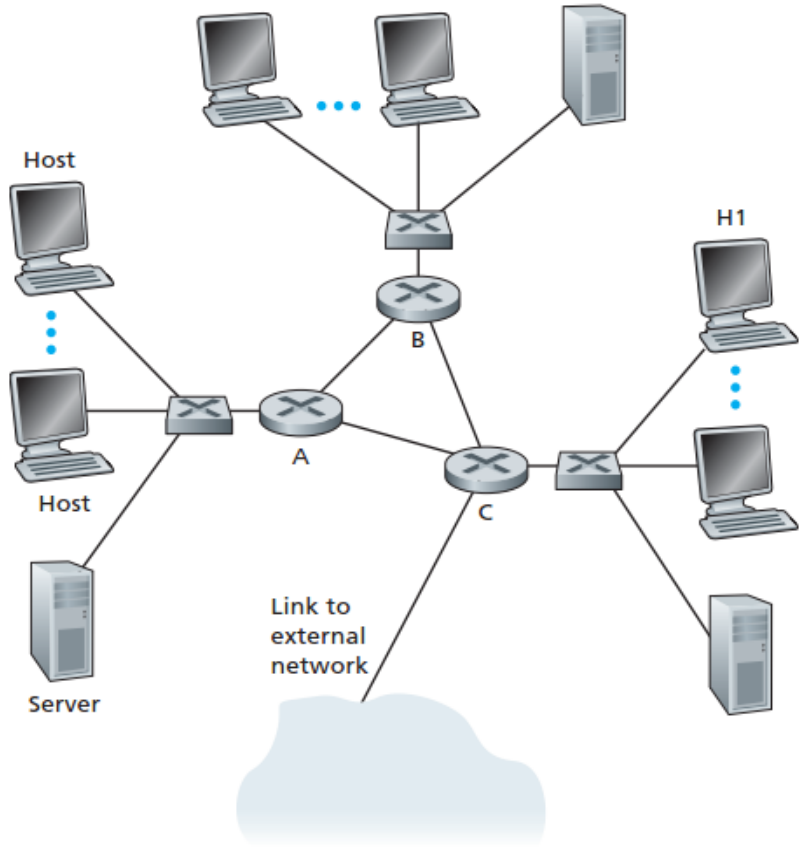


Figure 9.1 ♦ A simple scenario illustrating the uses of network management

Computer Networking, a Top-Down Approach, 6E

Simple Scenario

- Detecting failure of an interface card at a host or a router
- Host monitoring
- Monitoring traffic to aid in resource deployment
- Detecting rapid changes in routing tables
- Monitoring for Service Level Agreements (SLAs)
- Intrusion detection

The Functions of the Network Manager

- The ISO has created a network management model
- Useful for placing these scenarios in a more structured framework
- Five areas of network management are defined

The Functions of the Network Manager

FCAPS Model

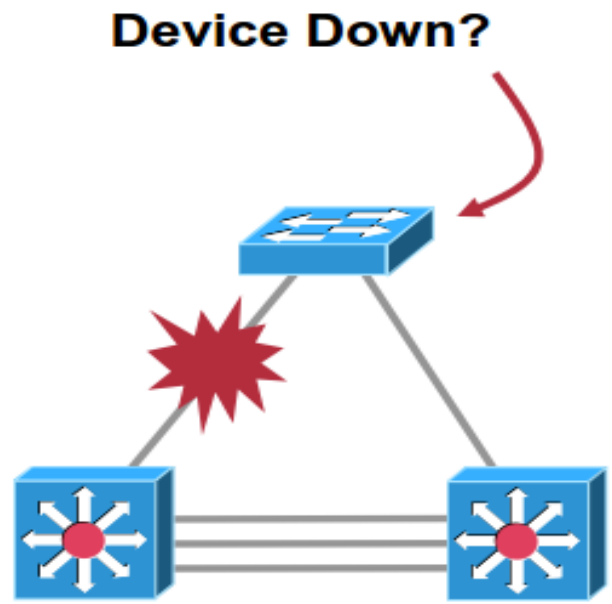
- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Fault Management

- Goal: to log, detect, and respond to fault conditions in the network
- How it is different from performance management?
- Fault management
  - the immediate handling of transient network failures
- Performance management
  - the longer-term view of providing acceptable levels of performance in the face of varying traffic demands and occasional network device failures
- SNMP protocol plays a central role in fault management

Fault Management

- "The process of locating, diagnosing, and correcting network problems"
- Increases network reliability and effectiveness
- More than just "firefighting"
- Increases the productivity of network users



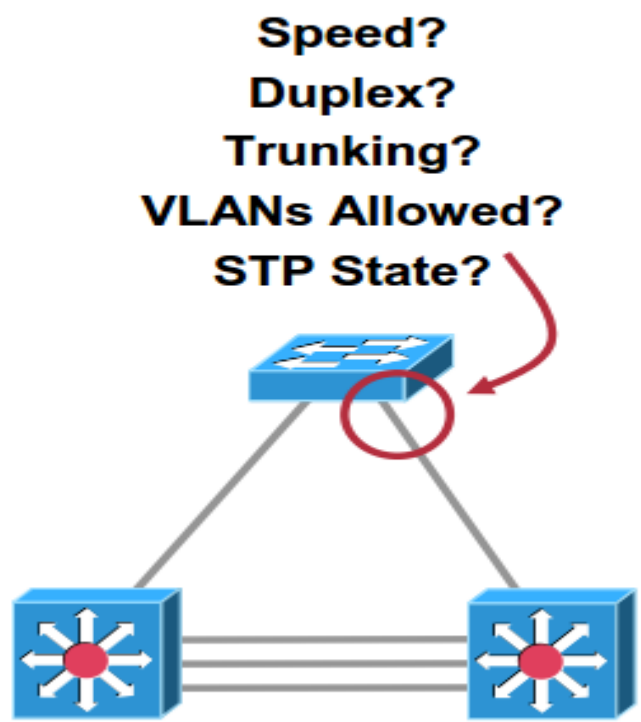
Fault Management

Steps for Successful Fault Management:

- Identify the problem by gathering information about the state of the network (polling and trap generation)
- Restore any services that have been lost
- Isolate the cause and decide if the fault should be managed
- Correct the fault if possible

Configuration Management

- "The process of obtaining data from the network and using that data to manage the setup of all network devices"
- Allows rapid access to configuration information
- Facilitates remote configuration and provisioning
- Provides an up-to-date inventory of network components



Configuration Management

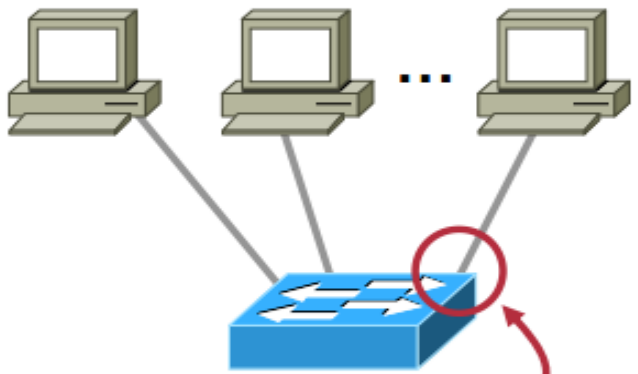
Cisco.com

Steps for Successful Configuration Management:

- Gather current network configuration (either manually or automatically)
- Use that data to modify network device configuration in order to provision the network
- Store the configuration data and maintain an up-to-date inventory of all network components
- Produce various inventory reports

Accounting Management

- "Measuring the usage of network resources by users in order to establish the metrics, check quotas, determine costs, and bill users"
- Measures and reports accounting information based on individual groups and users
- Administers the cost of the network
- Internal verification of third-party billing for usage



Input Octets?

Output Octets?

Total Broadcasts?

Accounting Management

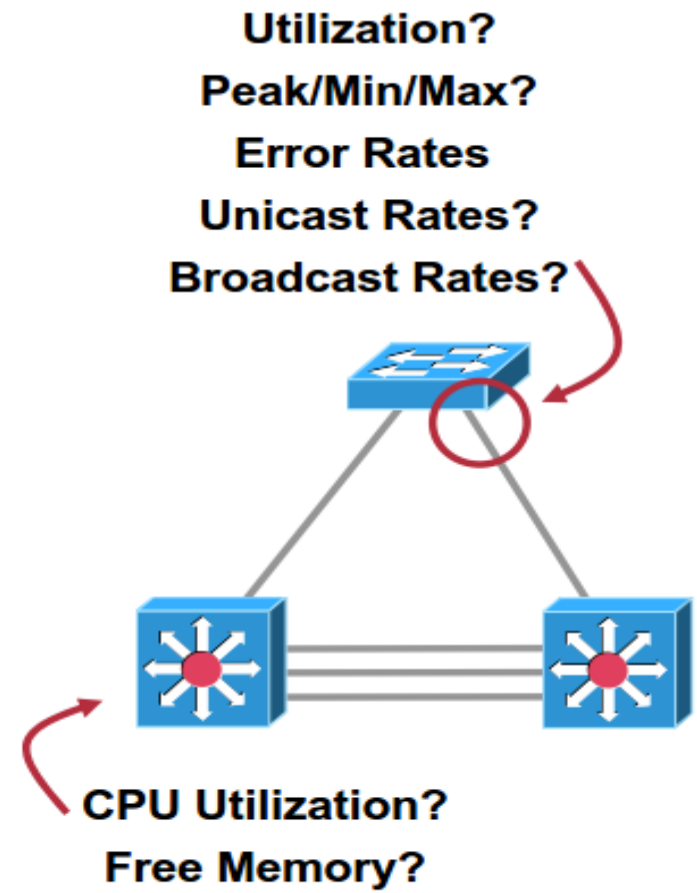
Cisco.com

Address the Different Steps Involved for Accounting Management:

- Gather network resource utilization information
- Use metrics to set usage quotas
- Billing users for their network use
- Consider the cost of accounting

Performance Management

- "Ensuring that the data network remains accessible and as uncongested as possible"
- Reduces network overcrowding and inaccessibility
- Provides a consistent level of service to the network user
- Determine utilization trends to proactively isolate and solve performance problems



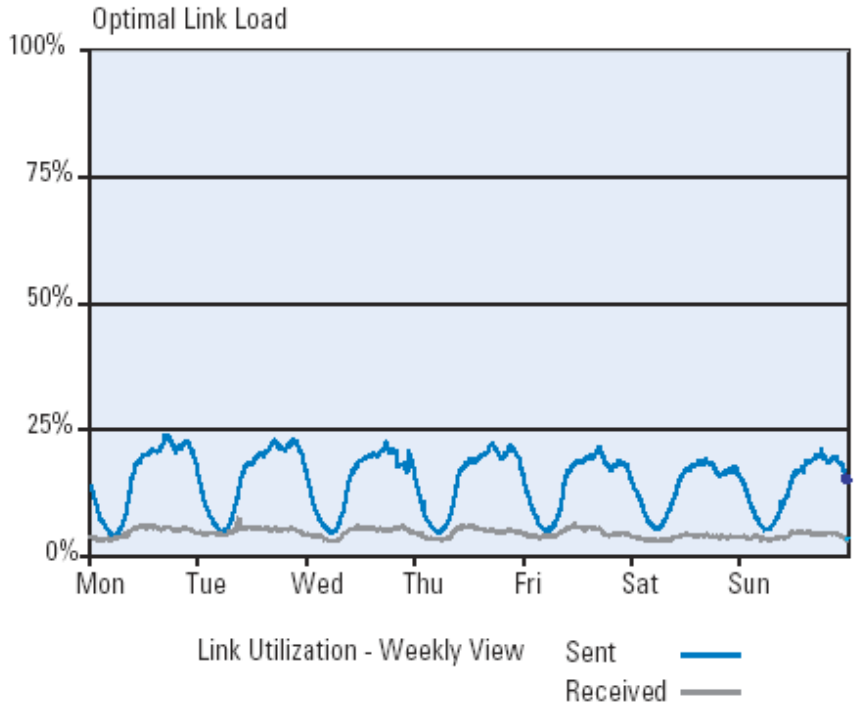
Performance Management

Steps for Successful Performance Management:

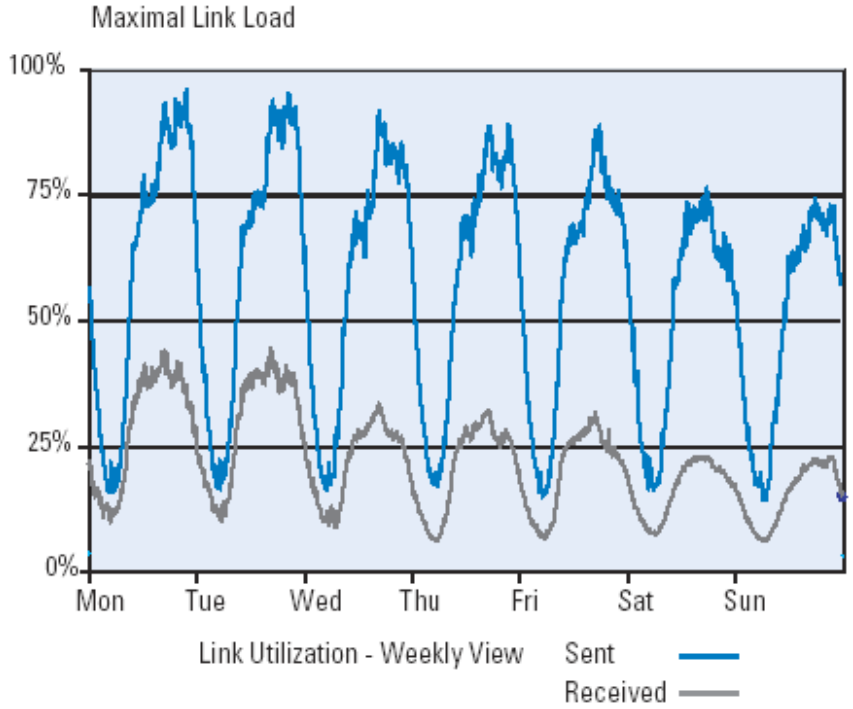
- Collect data on current network link and device utilization
- Baseline the utilization metrics and isolate any existing performance problems
- Set utilization thresholds based on the baseline
- Analyze the historical data for recognizing trends
- Resource planning and tuning
- Remember—measuring performance impacts performance

Performance Management

Relative Link Loading — An Optimally Loaded Link



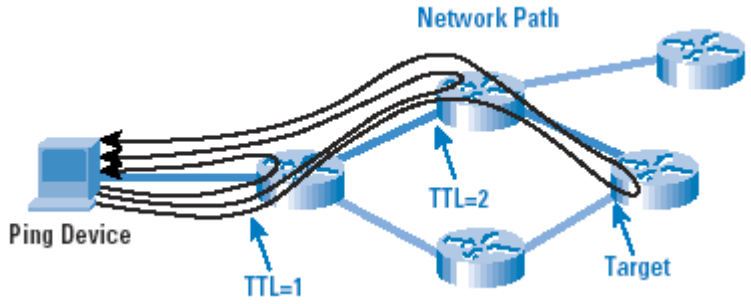
Relative Link Loading — A Maximally Loaded Link



http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/measuring_ip.html

Performance Management

Ping Path



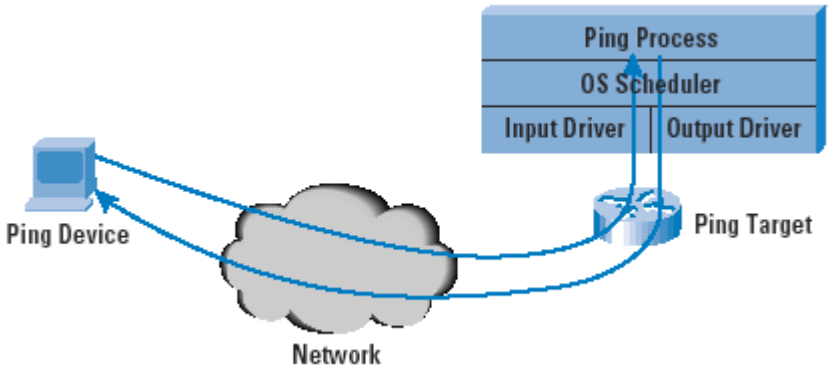
Ping Report

```
% ping www.iab.org
PING www.iab.org (132.151.6.25): 56 data bytes
64 bytes from 132.151.6.25: icmp_seq=0 ttl=44 time=254.409 ms
64 bytes from 132.151.6.25: icmp_seq=1 ttl=44 time=254.197 ms
64 bytes from 132.151.6.25: icmp_seq=2 ttl=44 time=255.238 ms
64 bytes from 132.151.6.25: icmp_seq=3 ttl=44 time=255.874 ms
--- www.iab.org ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 254.197/254.930/255.874/0.670 ms
```

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/measuring_ip.html

Performance Management

Traceroute Path



Traceroute Report

```
% traceroute www.cisco.com
traceroute to www.cisco.com (198.133.219.25), 64 hops max, 40 byte packets
1  dickson-gw1.Canberra.telstra.net (203.50.0.1)  0.272 ms  0.265 ms  0.270 ms
2  GigabitEthernet4-1.civ12.Canberra.telstra.net (203.50.8.1)  0.402 ms  0.272 ms  0.259 ms
3  GigabitEthernet3-1.civ-core2.Canberra.telstra.net (203.50.7.5)  0.214 ms  0.227 ms  0.193 ms
4  GigabitEthernet2-2.dkn-core1.Canberra.telstra.net (203.50.6.126)  0.459 ms  0.394 ms  0.385 ms
5  Pos4-0.ken-core4.Sydney.telstra.net (203.50.6.121)  3.806 ms  3.762  ms  3.770 ms
6  Pos2-0.pad-core4.Sydney.telstra.net (203.50.6.22) 3.907 ms  3.959 ms  3.913 ms
7  GigabitEthernet0-1.syd-core01.Sydney.net.reach.com (203.50.13.246)  3.898 ms  3.866 ms  3.977 ms
8  i-13-2.sjc-core01.net.reach.com (202.84.143.41)  191.361 ms  191.365 ms  191.341 ms
9  sl-st21-sj-6-1.sprintlink.net (144.223.242.1) 186.955 ms  186.851 ms  187.010 ms
10  sl-bb25-sj-5-1.sprintlink.net (144.232.20.73)  187.241 ms  187.337 ms  187.055 ms
11  sl-gw11-sj-10-0.sprintlink.net (144.232.3.134)  187.279 ms  186.898 ms  186.821 ms
12  sl-ciscopsn2-11-0-0.sprintlink.net (144.228.44.14)  187.572 ms  187.495 ms  187.620 ms
13  sjck-dirty-gw1.cisco.com (128.107.239.5)  184.533 ms  184.686 ms  184.694 ms
14  sjck-sdf-ciod-gw1.cisco.com (128.107.239.106)  184.676 ms  184.686 ms  184.644 ms

15  www.cisco.com (198.133.219.25)  185.017 ms 185.122 ms 185.019 ms
```

Notes:
1) There are interprovider handovers at hops 7, 9, and 13.
2) There is a sudden jump in response times at hop 8. The additional 182 ms of round-trip latency corresponds to a 36,000-km submarine cable path. This can be explained by the hop-7 to hop-8 segment, including a submarine cable path between Australia and the United States.

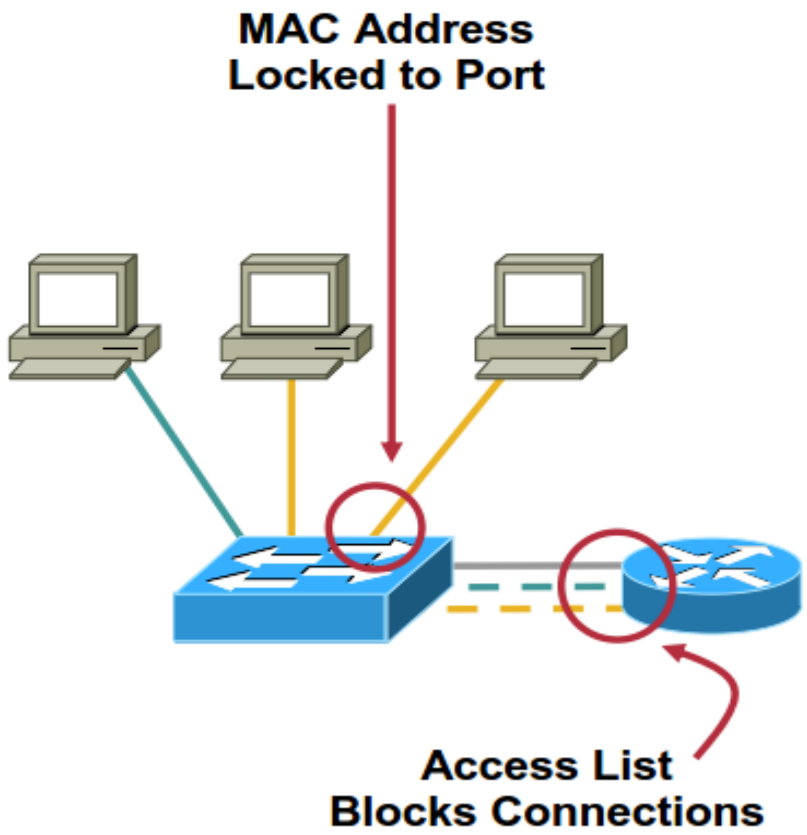
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/measuring_ip.html

Security Management

- Goal: to control access to network resources according to some well-defined policy
- For example, monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes
- Security management systems perform the following functions
  - identification of sensitive network resources
  - establishment of maps between sensitive network resources and user sets
  - mapping out which users can access which resources
  - monitoring of sensitive network access points
  - logging of inappropriate or failed access to these resources

Security Management

- "Protecting sensitive information on devices attached to a data network by controlling access points to that information"
- Builds network user confidence
- Secures sensitive information from both internal and external sources
- Protects the network functionality from malicious attacks



Security Management

Cisco.com

Steps for Successful Security Management:

- Identify sensitive information or devices
- Find the access points
- Secure the access points
- Protect the sensitive information by configuring encryption policies
- Implement a network intrusion detection scheme to enhance perimeter security

References

- James Kurose and Keith Ross, Computer Networking, a top-down approach, Pearson, 6E, 2013. Chapter 9.
- Cisco Systems, Introduction to Network Management, Session NMS-1N01, Networkers 2004.
- Geoff Huston, Measuring IP Network Performance, The Internet Protocol Journal, Cisco, Vol. 6, No. 1, 2003.
- Cisco Systems, Network Management System: Best Practices White Paper.
- Network Management Model, Lan switching first-step, Networking, eTutorials.org.