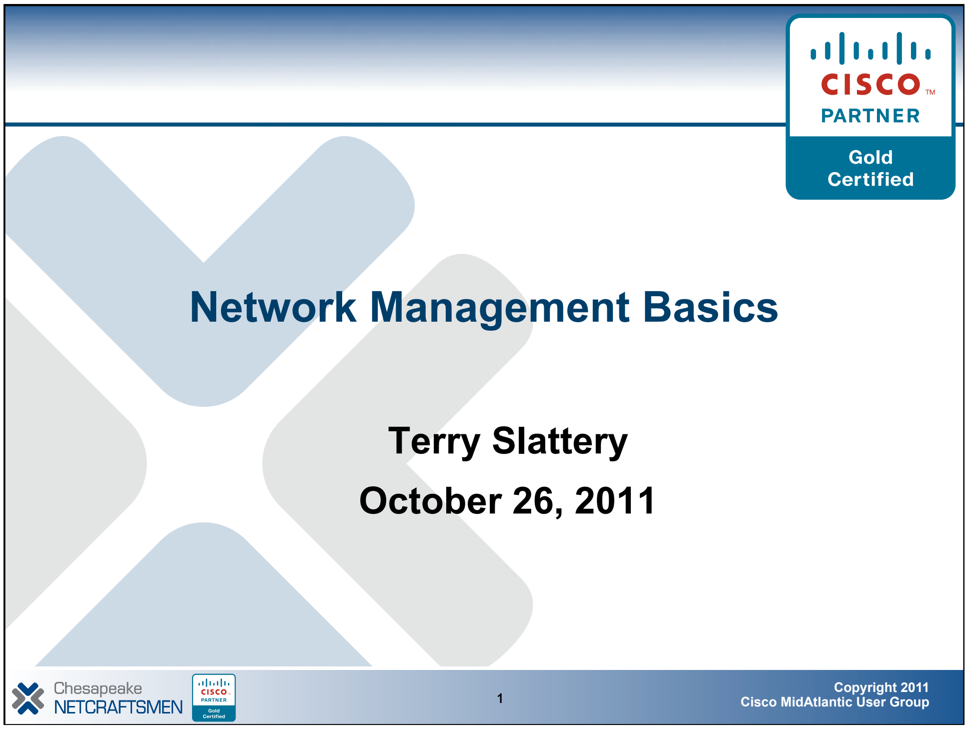
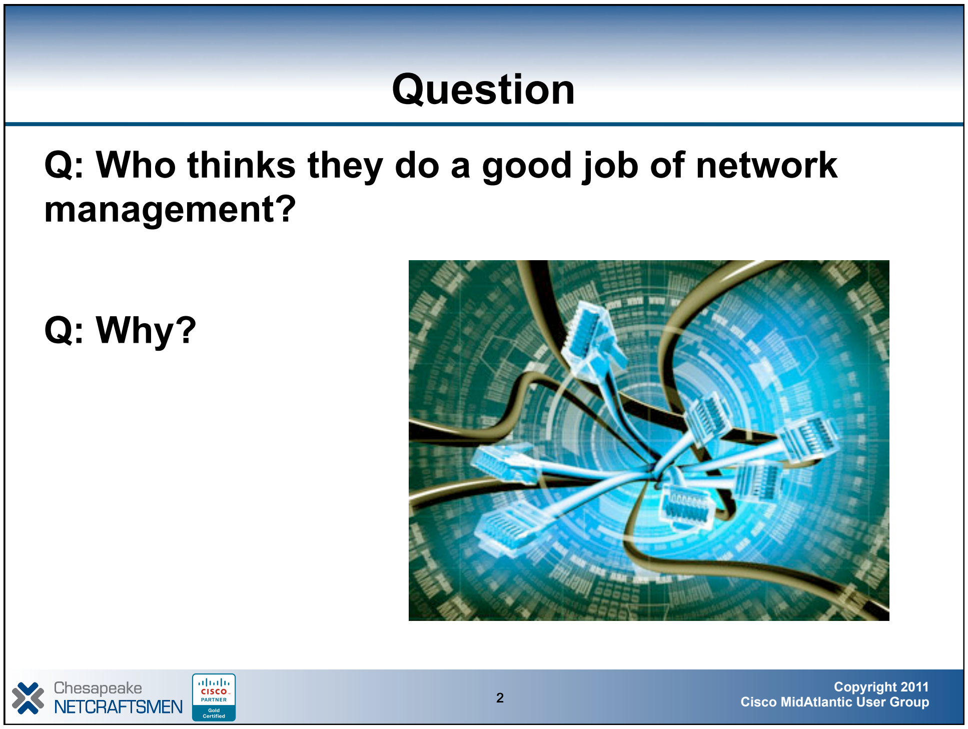


Network Management Basics

Terry Slattery

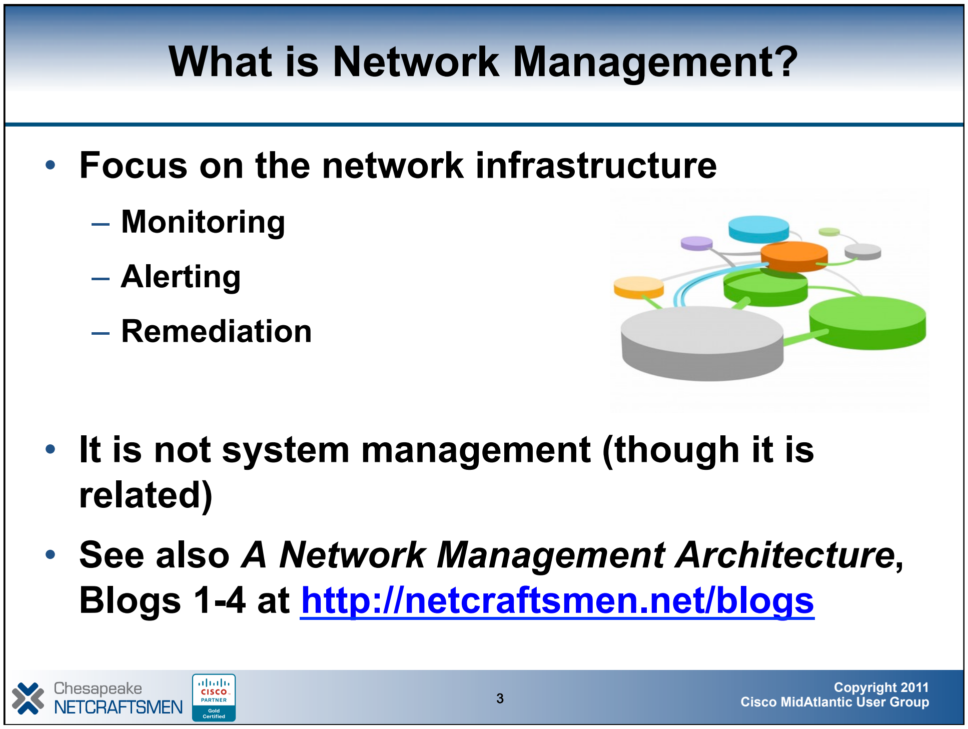
October 26, 2011



Question

Q: Who thinks they do a good job of network management?

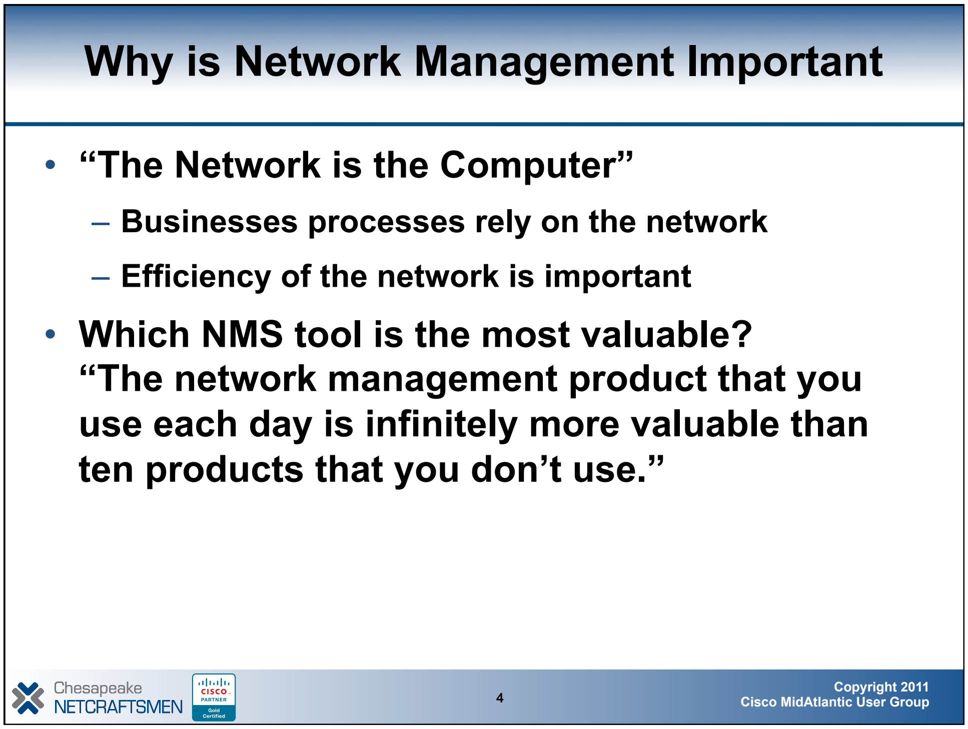
Q: Why?



What is Network Management?

- Focus on the network infrastructure
  - Monitoring
  - Alerting
  - Remediation
- It is not system management (though it is related)
- See also *A Network Management Architecture*, Blogs 1-4 at http://netcraftsmen.net/blogs

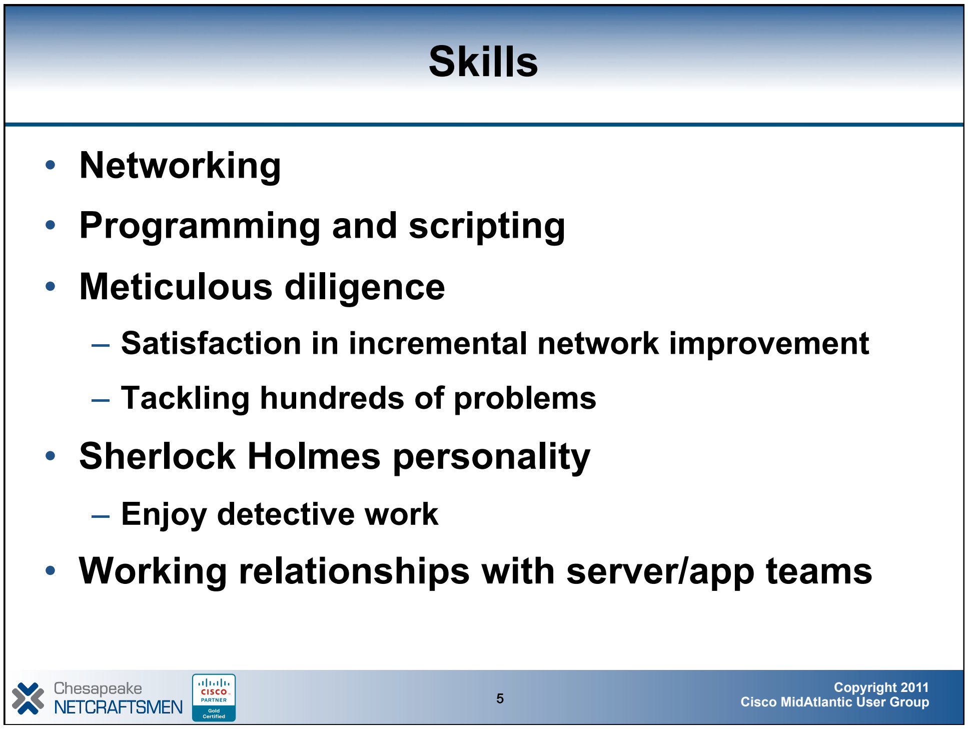
Chesapeake NETCRAFTSMEN 3 Copyright 2011 Cisco MidAtlantic User Group



Why is Network Management Important

- “The Network is the Computer”
  - Businesses processes rely on the network
  - Efficiency of the network is important
- Which NMS tool is the most valuable? “The network management product that you use each day is infinitely more valuable than ten products that you don’t use.”

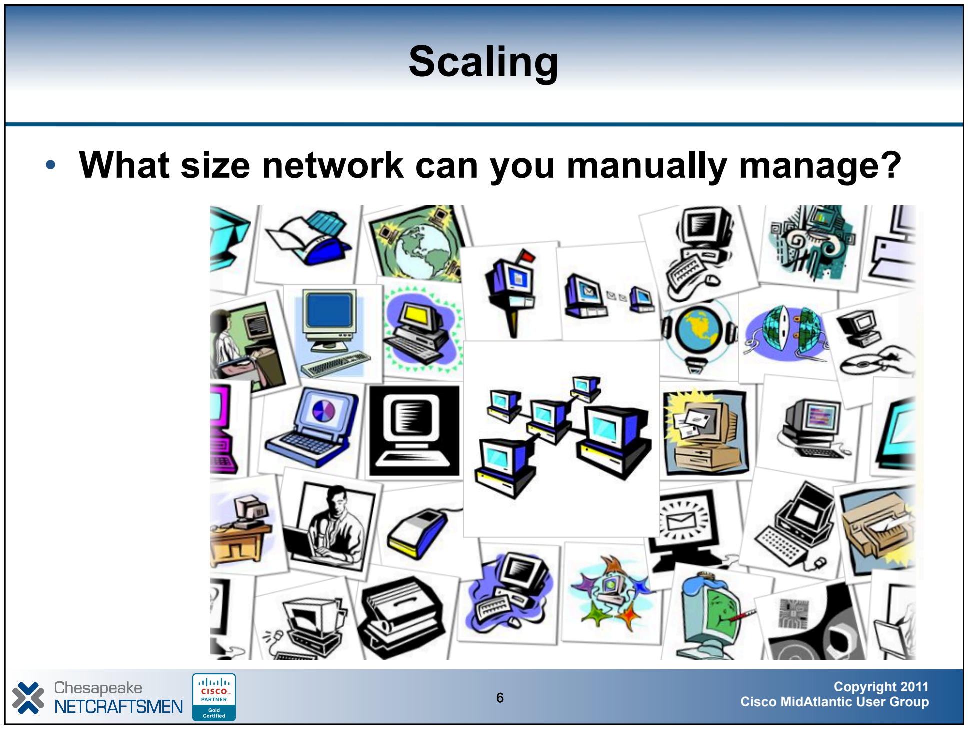
Chesapeake NETCRAFTSMEN 4 Copyright 2011 Cisco MidAtlantic User Group



Skills

- Networking
- Programming and scripting
- Meticulous diligence
  - Satisfaction in incremental network improvement
  - Tackling hundreds of problems
- Sherlock Holmes personality
  - Enjoy detective work
- Working relationships with server/app teams

Chesapeake NETCRAFTSMEN 5 Copyright 2011 Cisco MidAtlantic User Group



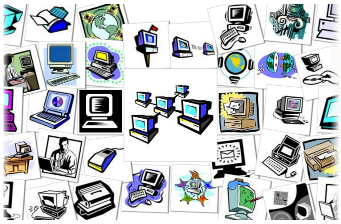
Scaling

- What size network can you manually manage?

Chesapeake NETCRAFTSMEN 6 Copyright 2011 Cisco MidAtlantic User Group

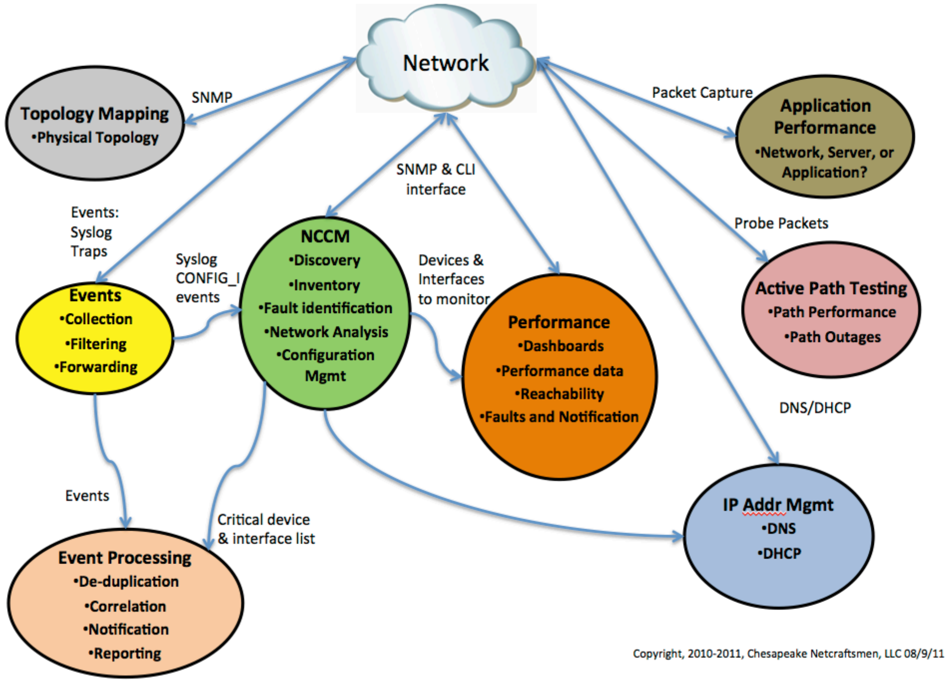
Scaling

- Automation is needed for most networks
- Manual methods for most processes don’t scale
  - Checking config consistency of 500 routers and switches
  - Monitoring thousands of interfaces for errors
  - Path testing (e.g., IP SLA)
  - Maintaining network diagrams



Chesapeake NETCRAFTSMEN 7 Copyright 2011 Cisco MidAtlantic User Group

Network Management Architecture



Network

Topology Mapping
- •Physical Topology

SNMP

Events: Syslog Traps

Events
- •Collection
- •Filtering
- •Forwarding

Syslog CONFIG_I events

NCCM
- •Discovery
- •Inventory
- •Fault identification
- •Network Analysis
- •Configuration Mgmt

SNMP & CLI interface

Devices & Interfaces to monitor

Performance
- •Dashboards
- •Performance data
- •Reachability
- •Faults and Notification

Packet Capture

Application Performance
- •Network, Server, or Application?

Probe Packets

Active Path Testing
- •Path Performance
- •Path Outages

DNS/DHCP

IP Addr Mgmt
- •DNS
- •DHCP

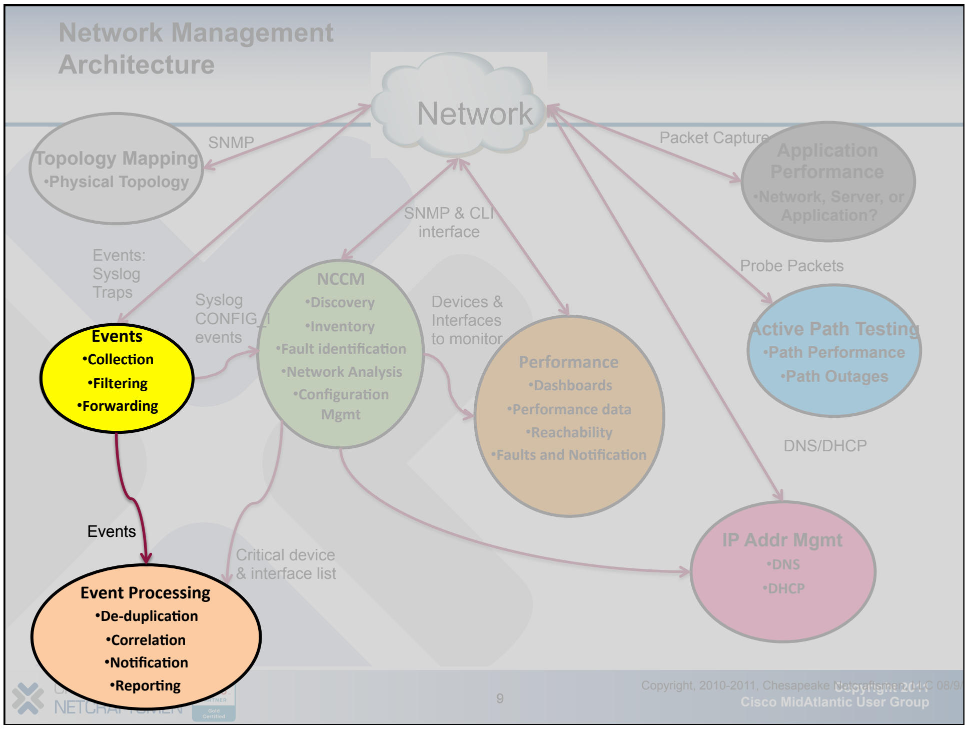
Events

Critical device & interface list

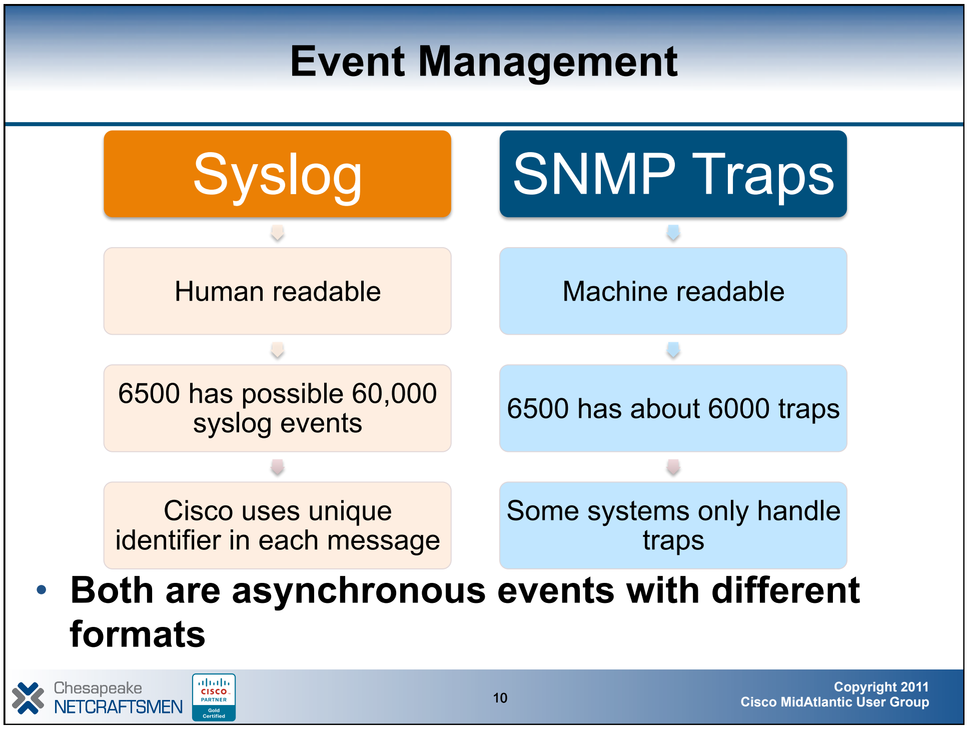
Event Processing
- •De-duplication
- •Correlation
- •Notification
- •Reporting

Copyright, 2010-2011, Chesapeake Netcraftsmen, LLC 08/9/11

Network Management Architecture



Event Management

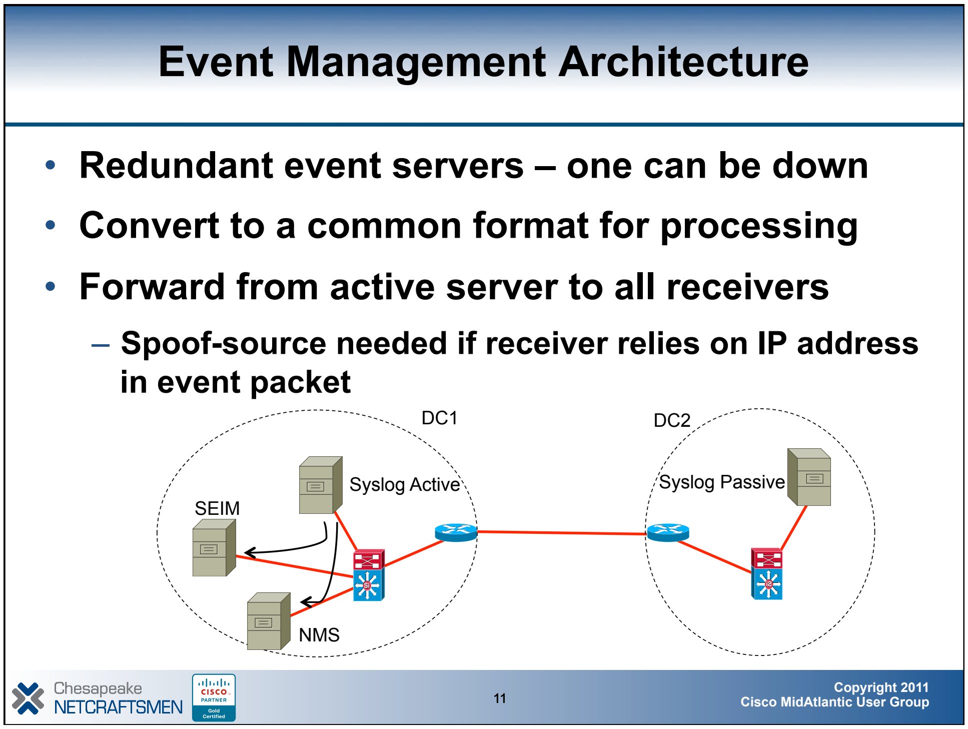


Syslog	SNMP Traps
Human readable	Machine readable
6500 has possible 60,000 syslog events	6500 has about 6000 traps
Cisco uses unique identifier in each message	Some systems only handle traps

- **Both are asynchronous events with different formats**

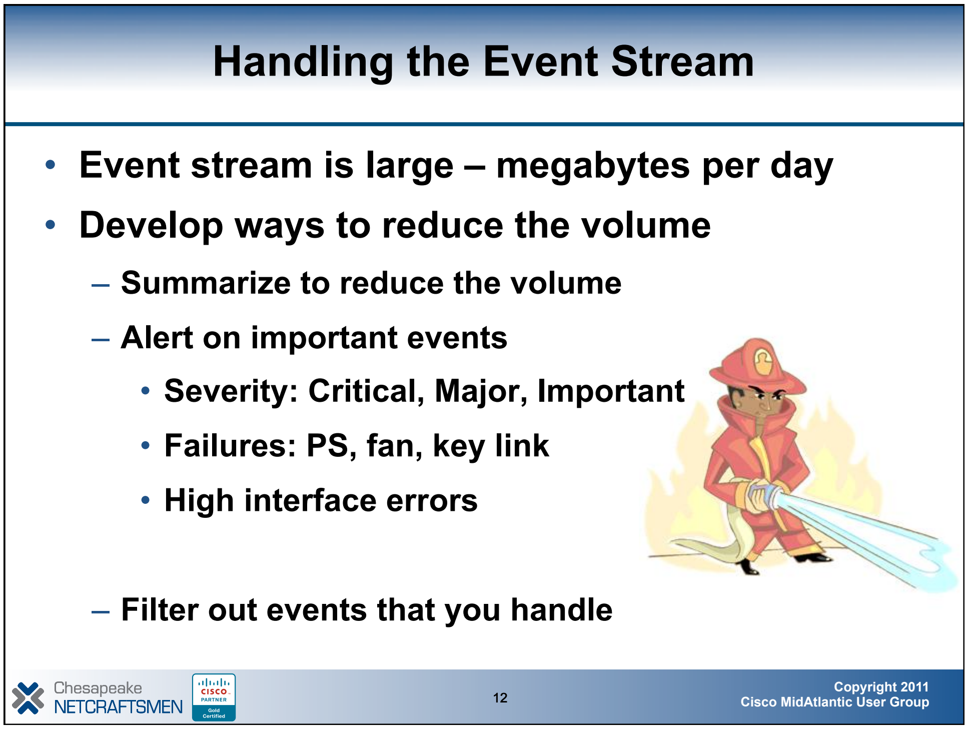
10

Copyright 2011
Cisco MidAtlantic User Group



Event Management Architecture

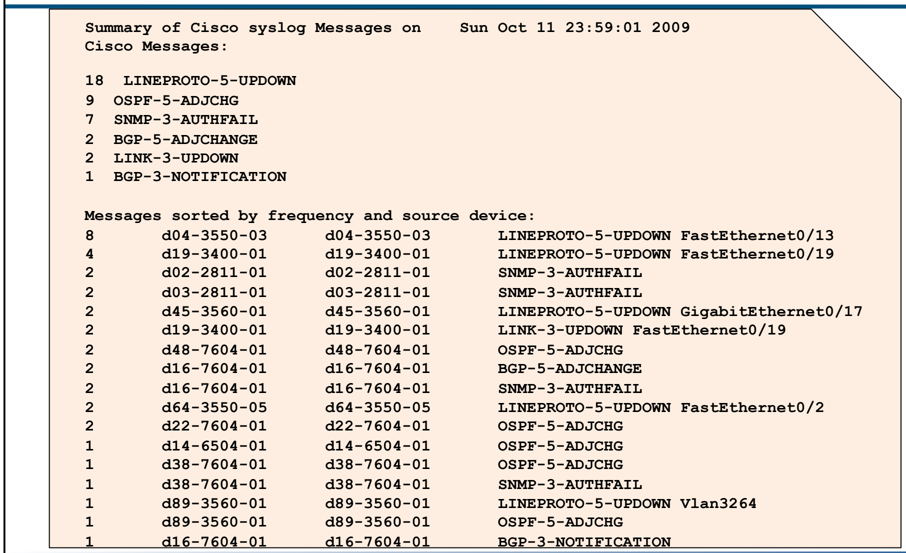
- Redundant event servers – one can be down
- Convert to a common format for processing
- Forward from active server to all receivers
  - Spoof-source needed if receiver relies on IP address in event packet



Handling the Event Stream

- Event stream is large – megabytes per day
- Develop ways to reduce the volume
  - Summarize to reduce the volume
  - Alert on important events
    - Severity: Critical, Major, Important
    - Failures: PS, fan, key link
    - High interface errors
  - Filter out events that you handle

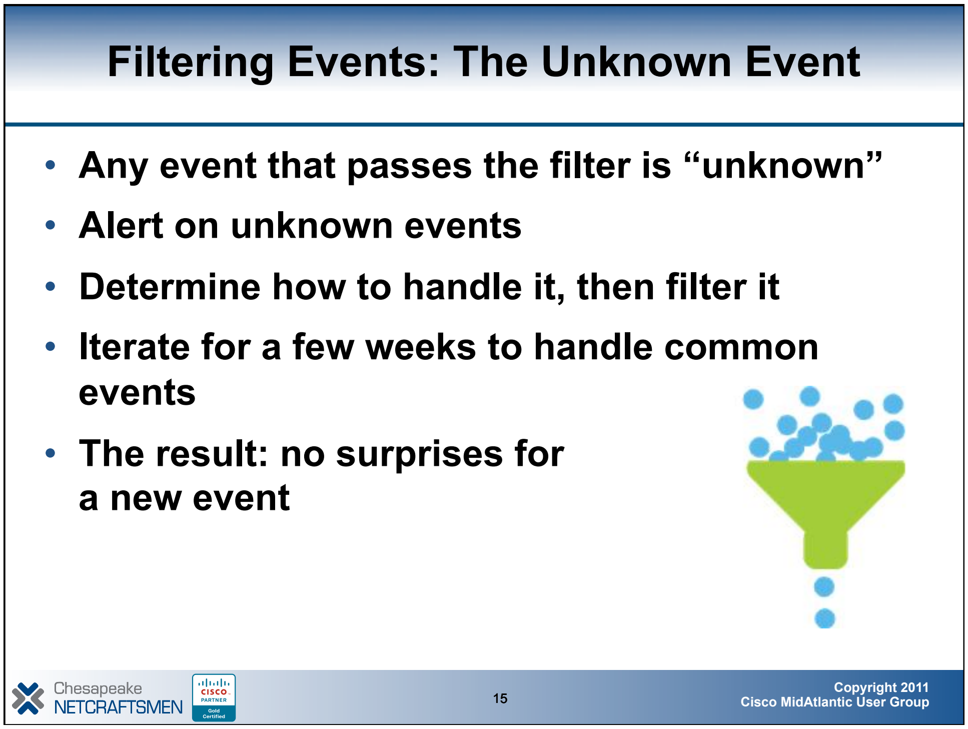
Syslog Summary



```
Summary of Cisco syslog Messages on    Sun Oct 11 23:59:01 2009
Cisco Messages:

18  LINEPROTO-5-UPDOWN
9  OSPF-5-ADJCHG
7  SNMP-3-AUTHFAIL
2  BGP-5-ADJCHANGE
2  LINK-3-UPDOWN
1  BGP-3-NOTIFICATION

Messages sorted by frequency and source device:
8       d04-3550-03      d04-3550-03      LINEPROTO-5-UPDOWN FastEthernet0/13
4       d19-3400-01      d19-3400-01      LINEPROTO-5-UPDOWN FastEthernet0/19
2       d02-2811-01      d02-2811-01      SNMP-3-AUTHFAIL
2       d03-2811-01      d03-2811-01      SNMP-3-AUTHFAIL
2       d45-3560-01      d45-3560-01      LINEPROTO-5-UPDOWN GigabitEthernet0/17
2       d19-3400-01      d19-3400-01      LINK-3-UPDOWN FastEthernet0/19
2       d48-7604-01      d48-7604-01      OSPF-5-ADJCHG
2       d16-7604-01      d16-7604-01      BGP-5-ADJCHANGE
2       d16-7604-01      d16-7604-01      SNMP-3-AUTHFAIL
2       d64-3550-05      d64-3550-05      LINEPROTO-5-UPDOWN FastEthernet0/2
2       d22-7604-01      d22-7604-01      OSPF-5-ADJCHG
1       d14-6504-01      d14-6504-01      OSPF-5-ADJCHG
1       d38-7604-01      d38-7604-01      OSPF-5-ADJCHG
1       d38-7604-01      d38-7604-01      SNMP-3-AUTHFAIL
1       d89-3560-01      d89-3560-01      LINEPROTO-5-UPDOWN Vlan3264
1       d89-3560-01      d89-3560-01      OSPF-5-ADJCHG
1       d16-7604-01      d16-7604-01      BGP-3-NOTIFICATION
```

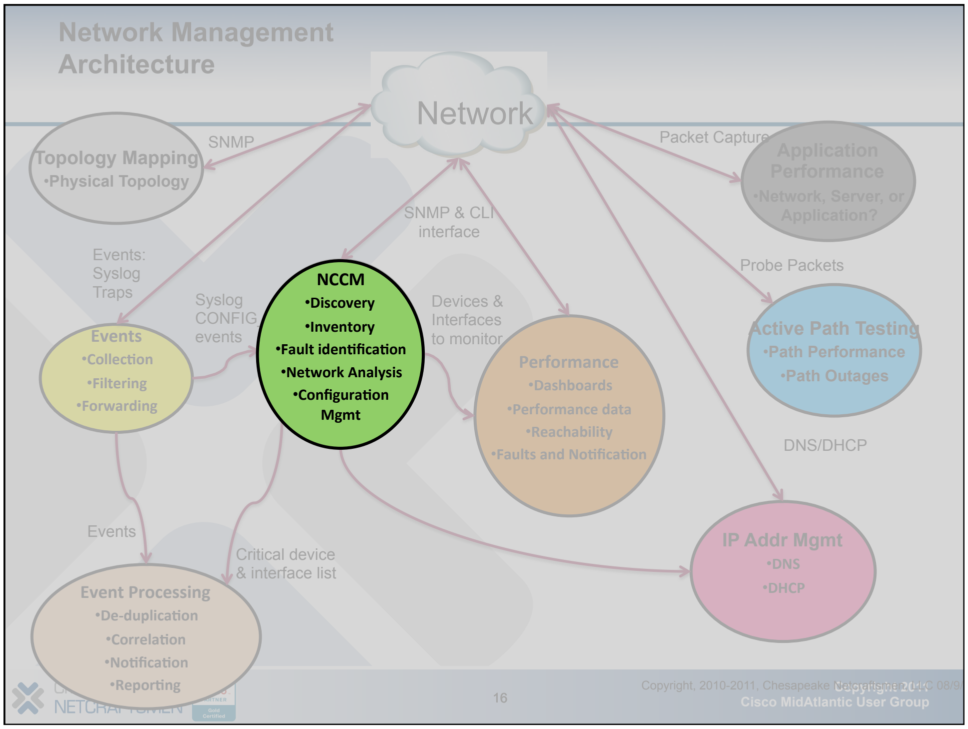
Filtering Events

- Sherlock Holmes, in *The Adventure of the Beryl Coronet*:
  It is an old maxim of mine that when you have excluded the impossible, whatever remains, however improbable, must be the truth.
- Filter out anything that you already handle or don't care about
  - Messages that generate alerts
  - Unimportant events (SNMP-3-AUTHFAIL)
  - Use `no logging event link-status`



Filtering Events: The Unknown Event

- Any event that passes the filter is “unknown”
- Alert on unknown events
- Determine how to handle it, then filter it
- Iterate for a few weeks to handle common events
- The result: no surprises for a new event



Network Management Architecture

Network

SNMP

Topology Mapping
- Physical Topology

Packet Capture

Application Performance
- Network, Server, or Application?

SNMP & CLI interface

Events: Syslog Traps

Probe Packets

Syslog CONFIG events

NCCM
- Discovery
- Inventory
- Fault identification
- Network Analysis
- Configuration Mgmt

Devices & Interfaces to monitor

Events
- Collection
- Filtering
- Forwarding

Performance
- Dashboards
- Performance data
- Reachability
- Faults and Notification

Active Path Testing
- Path Performance
- Path Outages

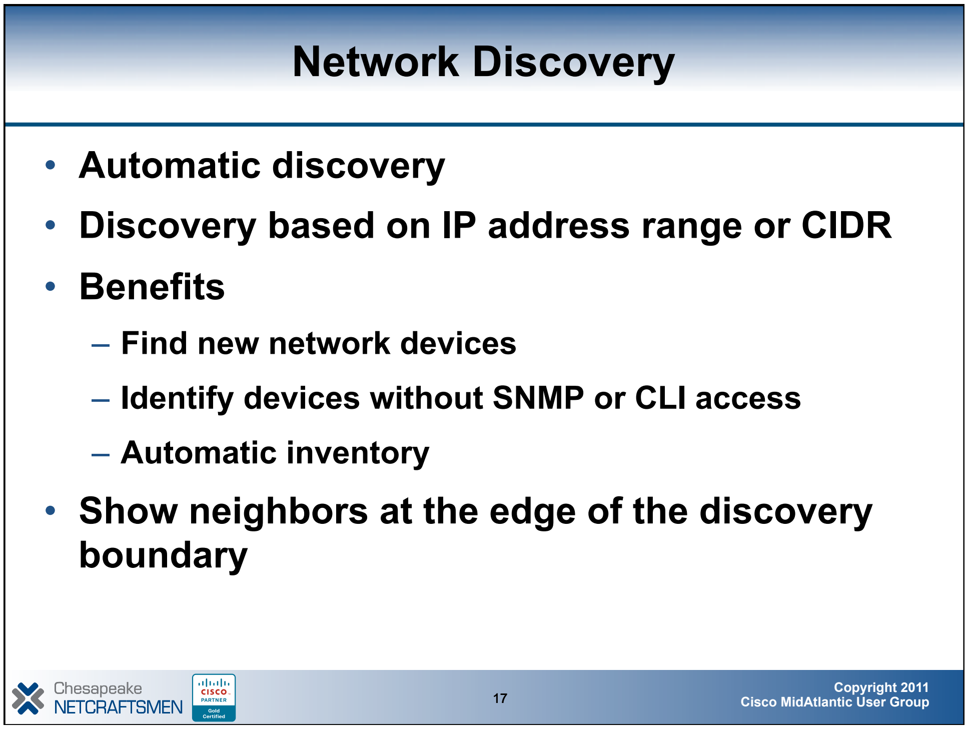
DNS/DHCP

Events

Critical device & interface list

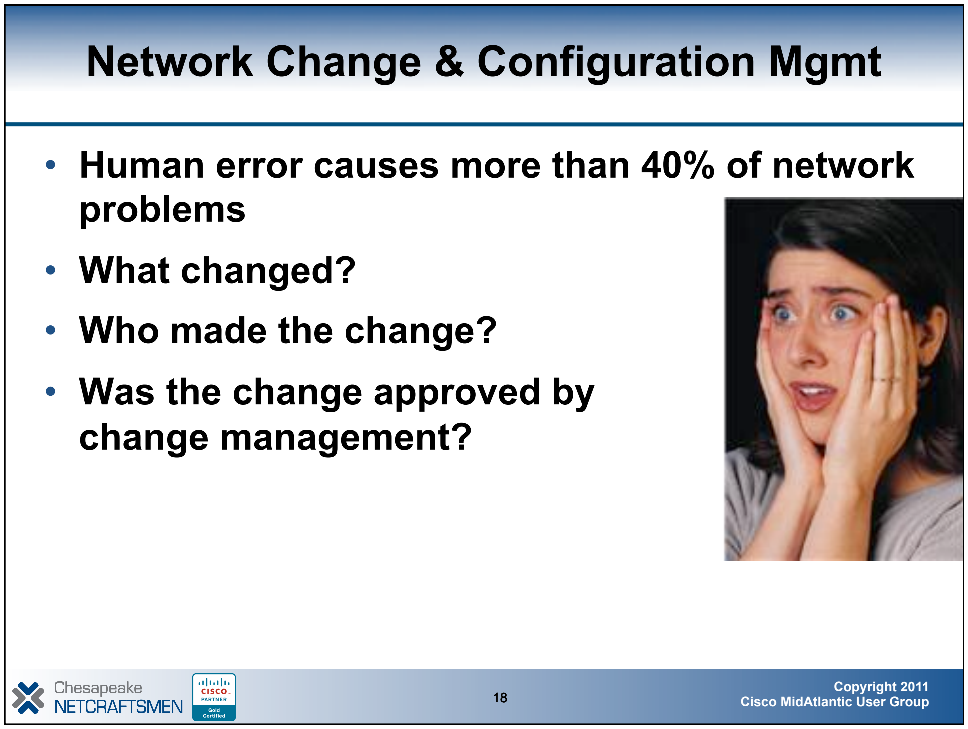
IP Addr Mgmt
- DNS
- DHCP

Event Processing
- De-duplication
- Correlation
- Notification
- Reporting



Network Discovery

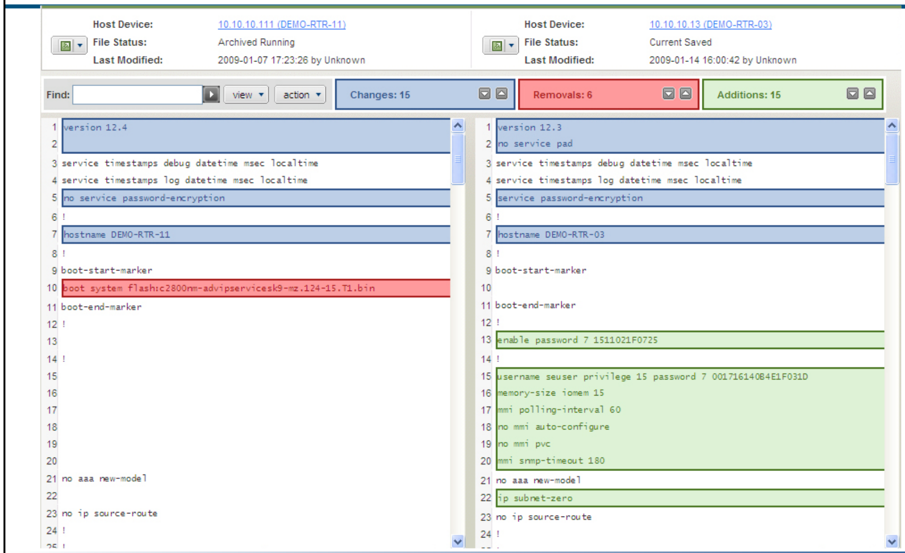
- Automatic discovery
- Discovery based on IP address range or CIDR
- Benefits
  - Find new network devices
  - Identify devices without SNMP or CLI access
  - Automatic inventory
- Show neighbors at the edge of the discovery boundary



Network Change & Configuration Mgmt

- Human error causes more than 40% of network problems
- What changed?
- Who made the change?
- Was the change approved by change management?

Comparing Two Device Configs



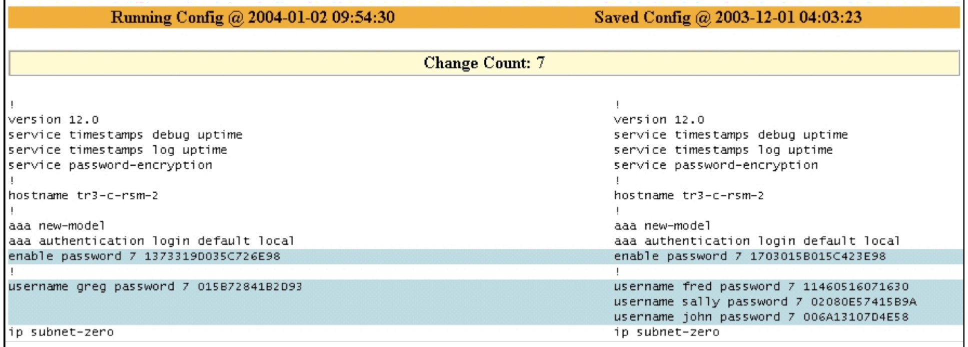
Host Device: 10.10.10.111 (DEMO-RTR-11)
File Status: Archived Running
Last Modified: 2009-01-07 17:23:26 by Unknown

Host Device: 10.10.10.13 (DEMO-RTR-03)
File Status: Current Saved
Last Modified: 2009-01-14 16:00:42 by Unknown

```
version 12.4

service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname DEMO-RTR-11
!
boot-start-marker
boot system flash:c2800nm-advipservicesk9-mz.124-15.T1.bin
boot-end-marker
!

!






no aaa new-model

no ip source-route
!
!
```

```
version 12.3
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname DEMO-RTR-03
!
boot-start-marker

boot-end-marker
!
enable password 7 1511021F0725
!
username seuser privilege 15 password 7 001716140B4E1F031D
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
no ip source-route
!
```

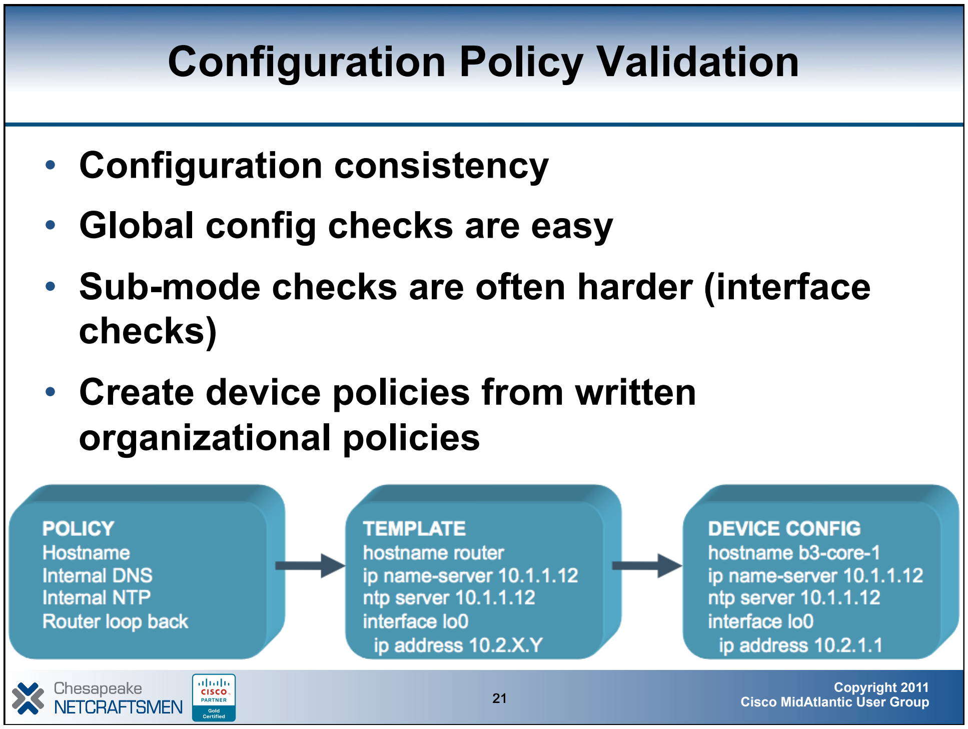
Comparing Running & Saved Configs



Running Config @ 2004-01-02 09:54:30	Saved Config @ 2003-12-01 04:03:23

Change Count: 7

```
!                                                     !
version 12.0                                          version 12.0
service timestamps debug uptime                       service timestamps debug uptime
service timestamps log uptime                         service timestamps log uptime
service password-encryption                           service password-encryption
!                                                     !
hostname tr3-c-rsm-2                                  hostname tr3-c-rsm-2
!                                                     !
aaa new-model                                         aaa new-model
aaa authentication login default local                aaa authentication login default local
enable password 7 1373319D035C726E98                  enable password 7 1703015B015C423E98
!                                                     !
username greg password 7 015B72841B2D93               username fred password 7 11460516071630
                                                      username sally password 7 02080E57415B9A
                                                      username john password 7 006A13107D4E58
ip subnet-zero                                        ip subnet-zero
```



Configuration Policy Validation

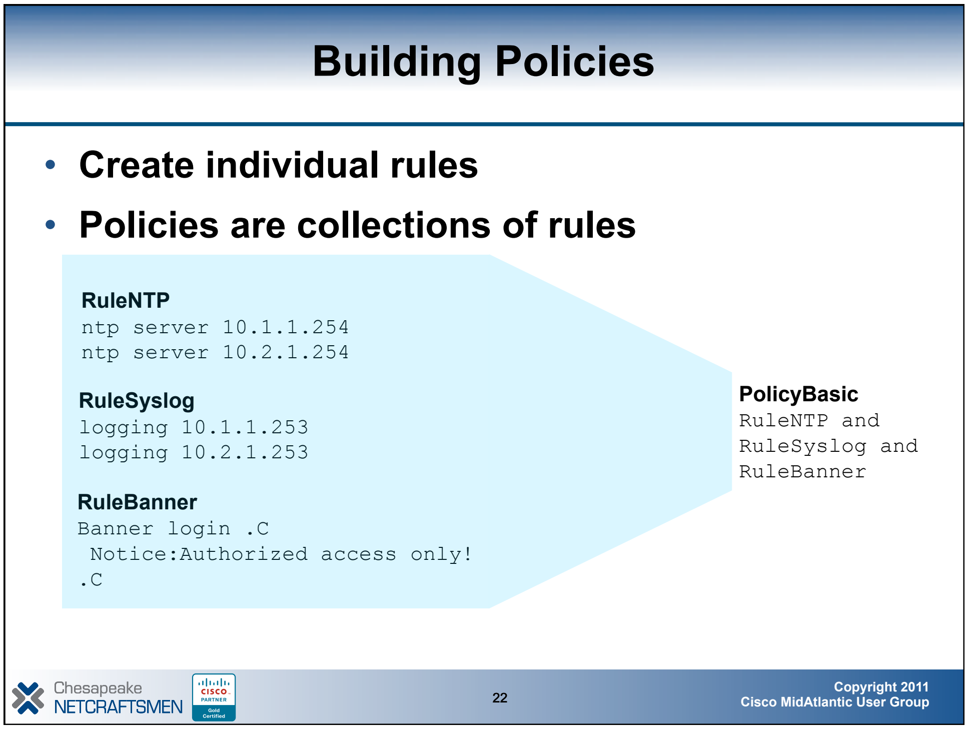
- Configuration consistency
- Global config checks are easy
- Sub-mode checks are often harder (interface checks)
- Create device policies from written organizational policies

POLICY
Hostname
Internal DNS
Internal NTP
Router loop back

TEMPLATE
hostname router
ip name-server 10.1.1.12
ntp server 10.1.1.12
interface lo0
 ip address 10.2.X.Y

DEVICE CONFIG
hostname b3-core-1
ip name-server 10.1.1.12
ntp server 10.1.1.12
interface lo0
 ip address 10.2.1.1

Chesapeake NETCRAFTSMEN 21 Copyright 2011
Cisco MidAtlantic User Group



Building Policies

- Create individual rules
- Policies are collections of rules

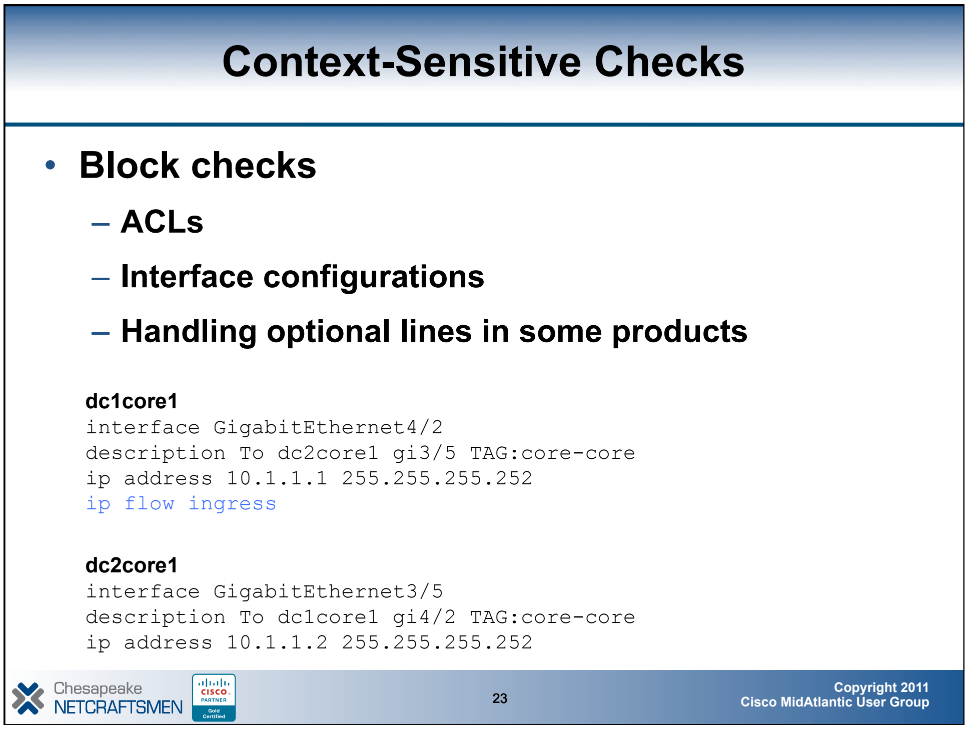
RuleNTP
```
ntp server 10.1.1.254
ntp server 10.2.1.254
```

RuleSyslog
```
logging 10.1.1.253
logging 10.2.1.253
```

RuleBanner
```
Banner login .C
 Notice:Authorized access only!
.C
```

PolicyBasic
```
RuleNTP and
RuleSyslog and
RuleBanner
```

Chesapeake NETCRAFTSMEN 22 Copyright 2011
Cisco MidAtlantic User Group



Context-Sensitive Checks

- Block checks
  - ACLs
  - Interface configurations
  - Handling optional lines in some products

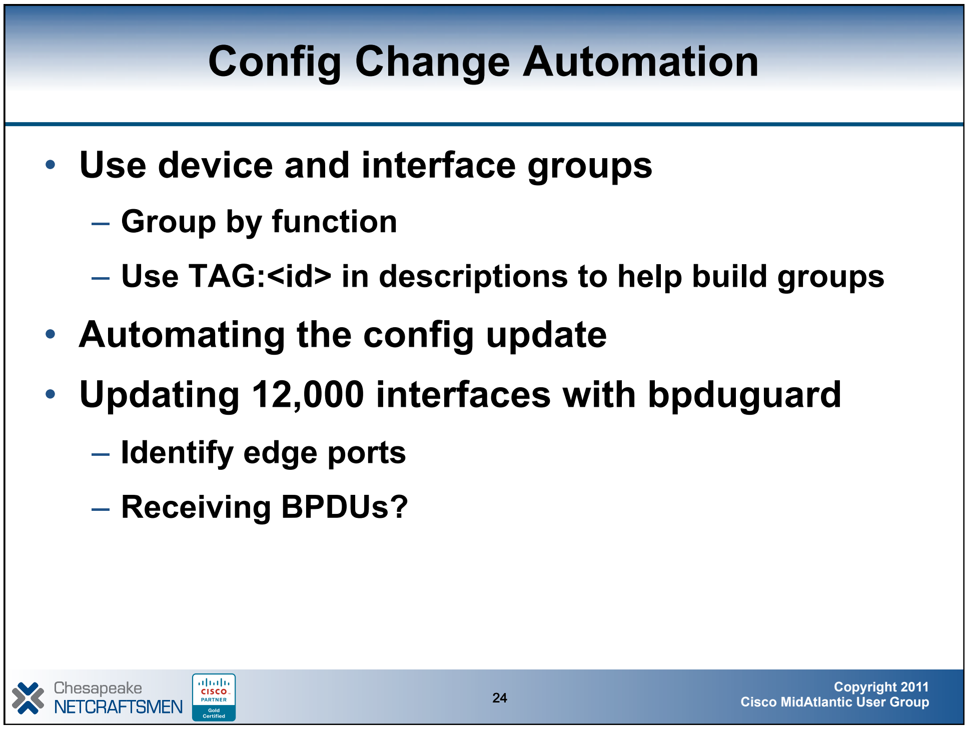
dc1core1

```
interface GigabitEthernet4/2
description To dc2core1 gi3/5 TAG:core-core
ip address 10.1.1.1 255.255.255.252
ip flow ingress
```

dc2core1

```
interface GigabitEthernet3/5
description To dc1core1 gi4/2 TAG:core-core
ip address 10.1.1.2 255.255.255.252
```

Chesapeake NETCRAFTSMEN 23 Copyright 2011 Cisco MidAtlantic User Group



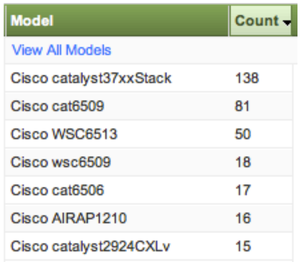
Config Change Automation

- Use device and interface groups
  - Group by function
  - Use TAG:<id> in descriptions to help build groups
- Automating the config update
- Updating 12,000 interfaces with bpduguard
  - Identify edge ports
  - Receiving BPDUs?

Chesapeake NETCRAFTSMEN 24 Copyright 2011 Cisco MidAtlantic User Group

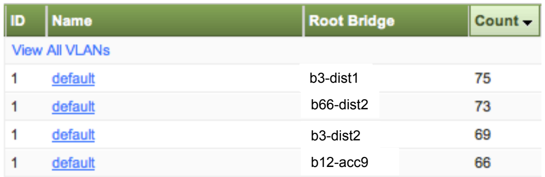
NCCM - Additional analysis

- Inventory of devices & modules
- Subnet utilization
- Subnet mask inconsistent

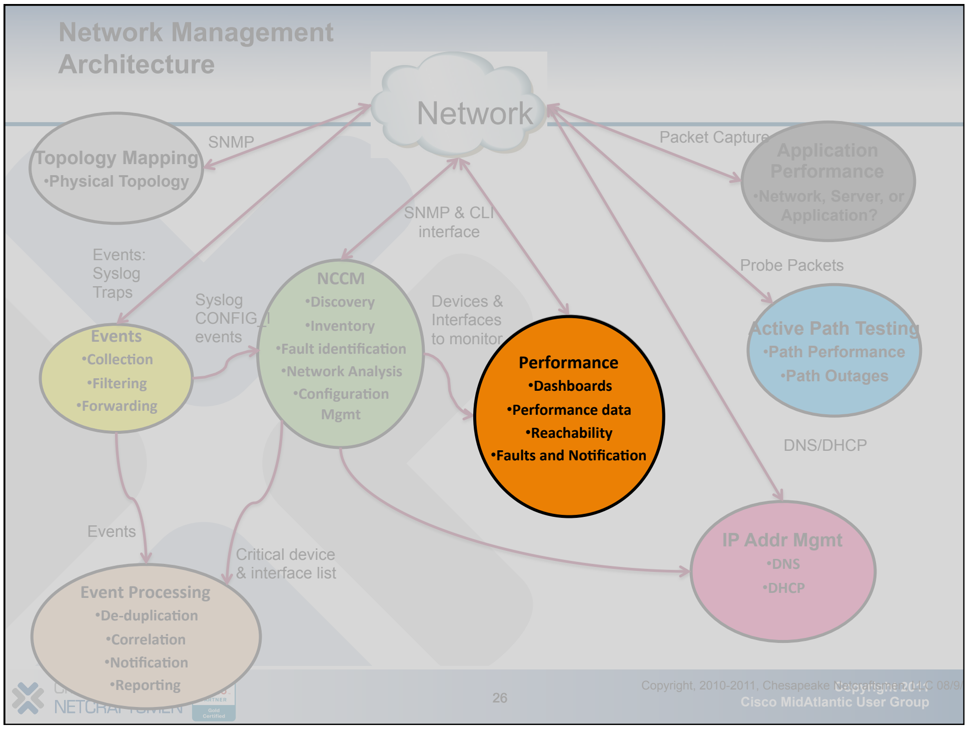


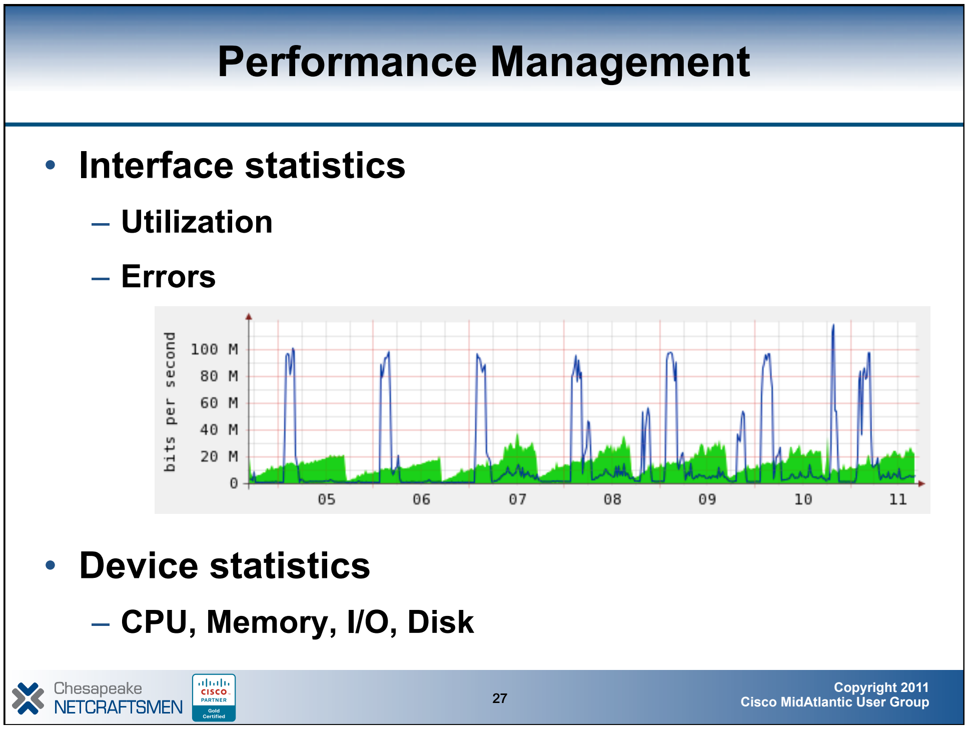
Model	Count
View All Models	
Cisco catalyst37xxStack	138
Cisco cat6509	81
Cisco WSC6513	50
Cisco wsc6509	18
Cisco cat6506	17
Cisco AIRAP1210	16
Cisco catalyst2924CXLv	15

- Spanning tree size (cannot do from configs alone)



ID	Name	Root Bridge	Count
View All VLANs			
1	default	b3-dist1	75
1	default	b66-dist2	73
1	default	b3-dist2	69
1	default	b12-acc9	66

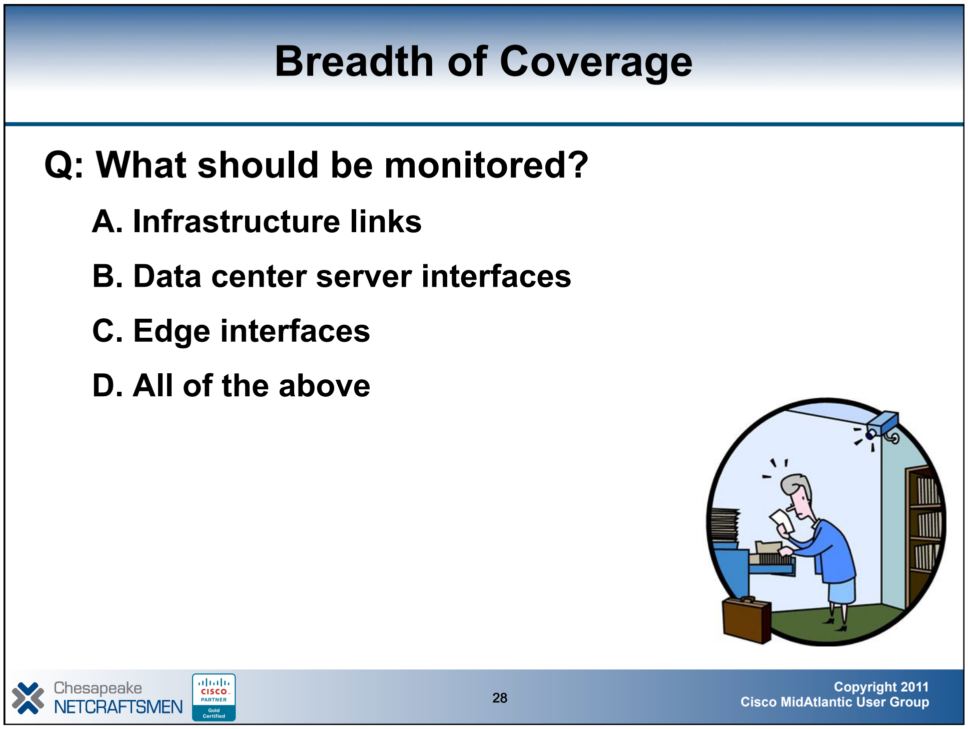




Performance Management

- **Interface statistics**
  - **Utilization**
  - **Errors**

- **Device statistics**
  - **CPU, Memory, I/O, Disk**



Breadth of Coverage

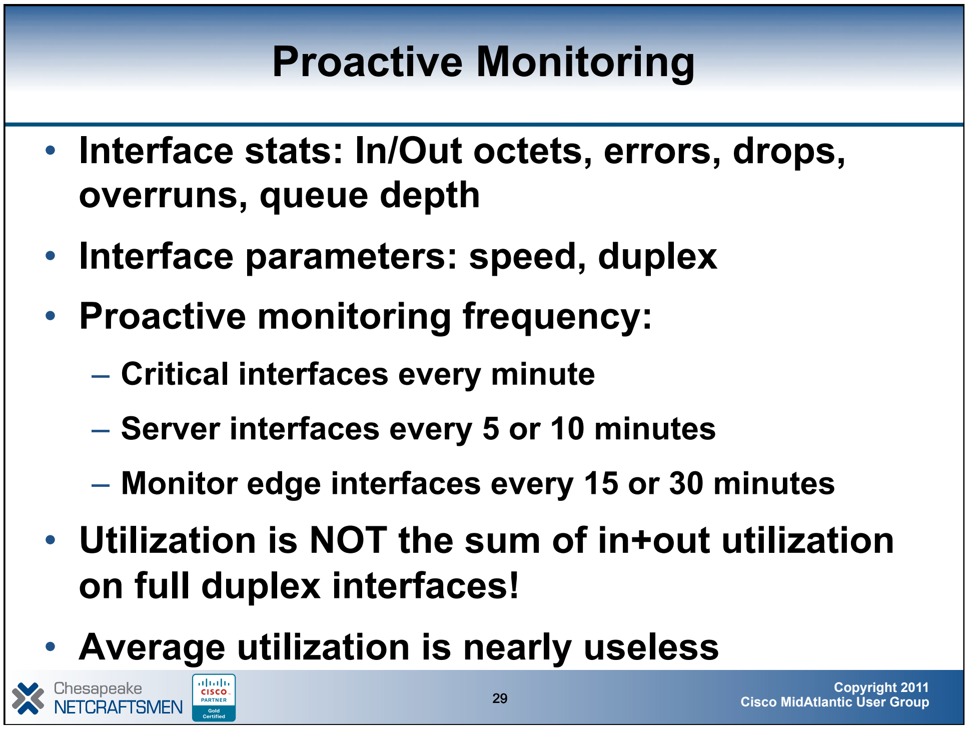
Q: What should be monitored?

A. Infrastructure links

B. Data center server interfaces

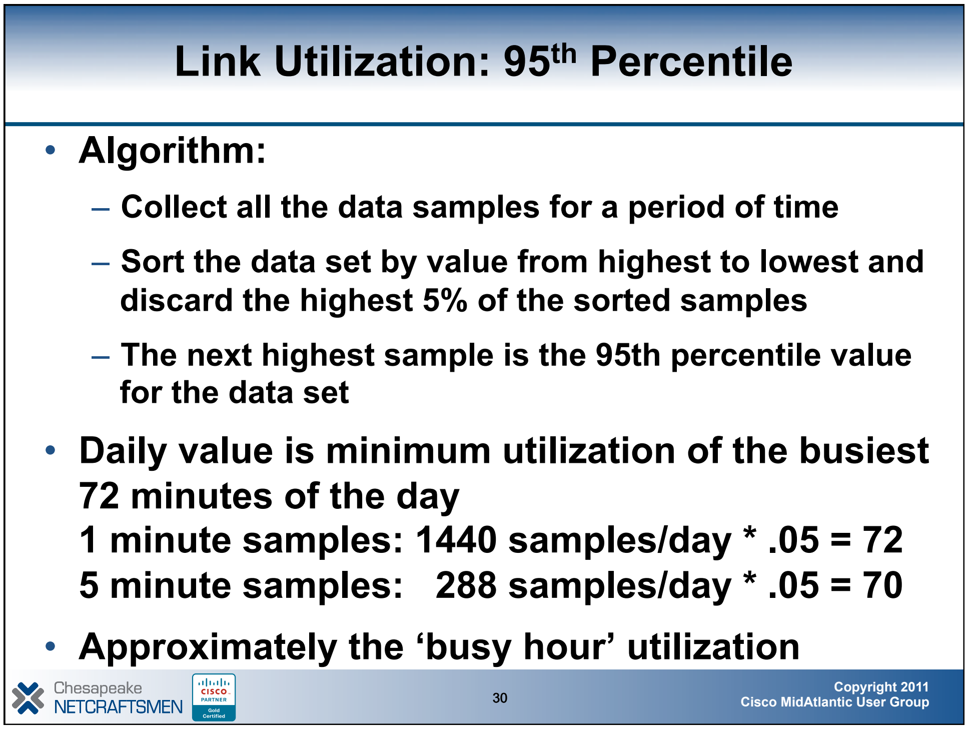
C. Edge interfaces

D. All of the above



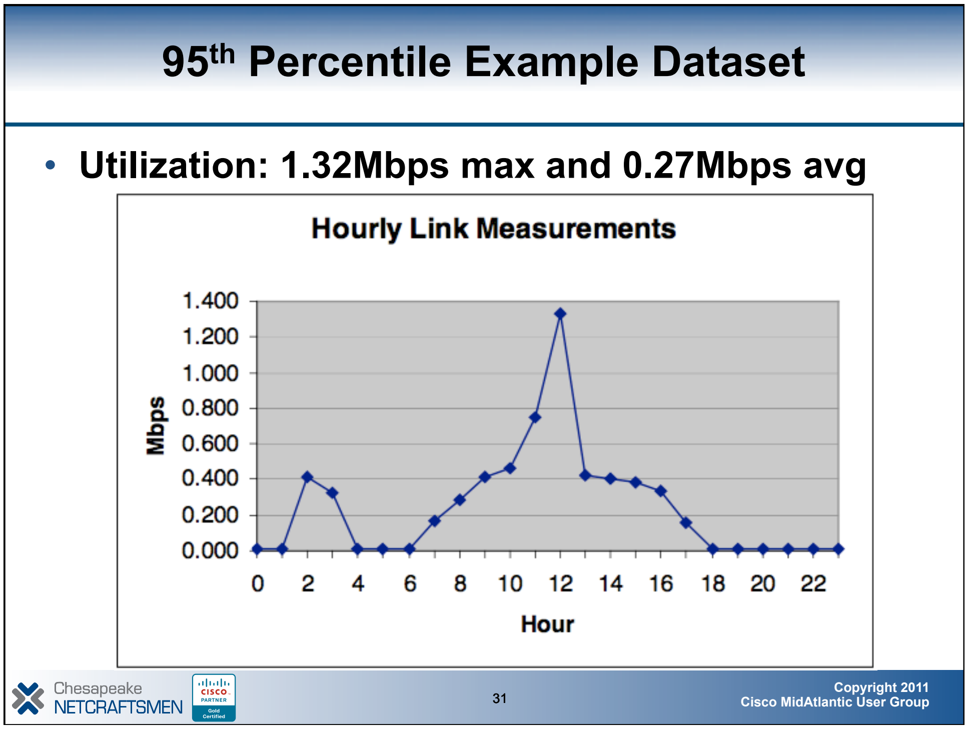
Proactive Monitoring

- Interface stats: In/Out octets, errors, drops, overruns, queue depth
- Interface parameters: speed, duplex
- Proactive monitoring frequency:
  - Critical interfaces every minute
  - Server interfaces every 5 or 10 minutes
  - Monitor edge interfaces every 15 or 30 minutes
- Utilization is NOT the sum of in+out utilization on full duplex interfaces!
- Average utilization is nearly useless



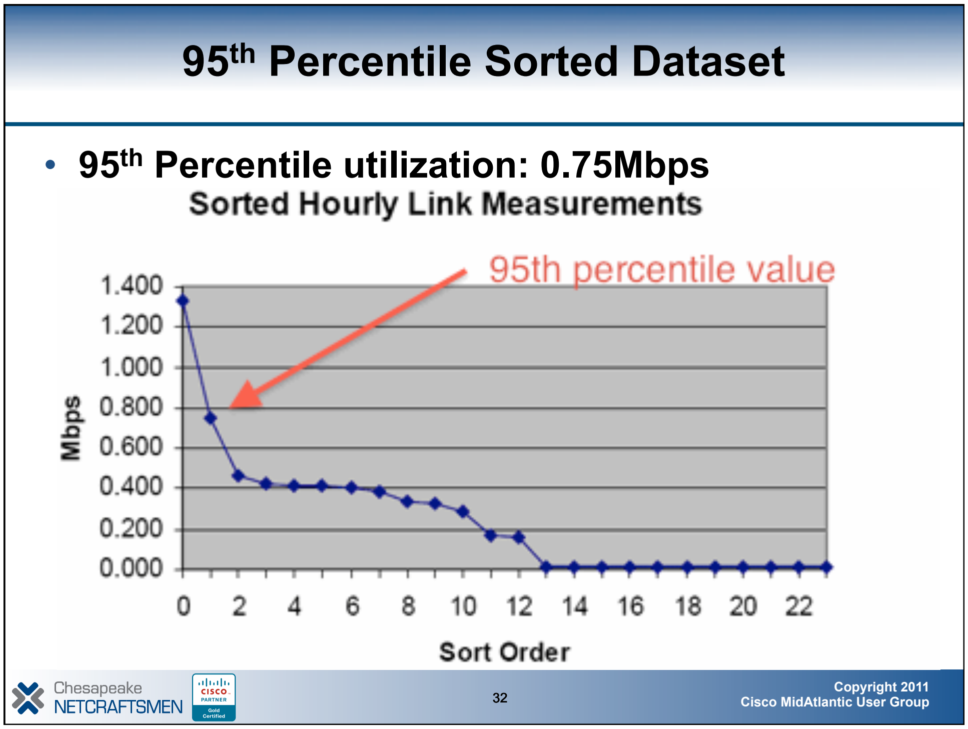
Link Utilization: 95th Percentile

- Algorithm:
  - Collect all the data samples for a period of time
  - Sort the data set by value from highest to lowest and discard the highest 5% of the sorted samples
  - The next highest sample is the 95th percentile value for the data set
- Daily value is minimum utilization of the busiest 72 minutes of the day
  1 minute samples: 1440 samples/day * .05 = 72
  5 minute samples: 288 samples/day * .05 = 70
- Approximately the ‘busy hour’ utilization



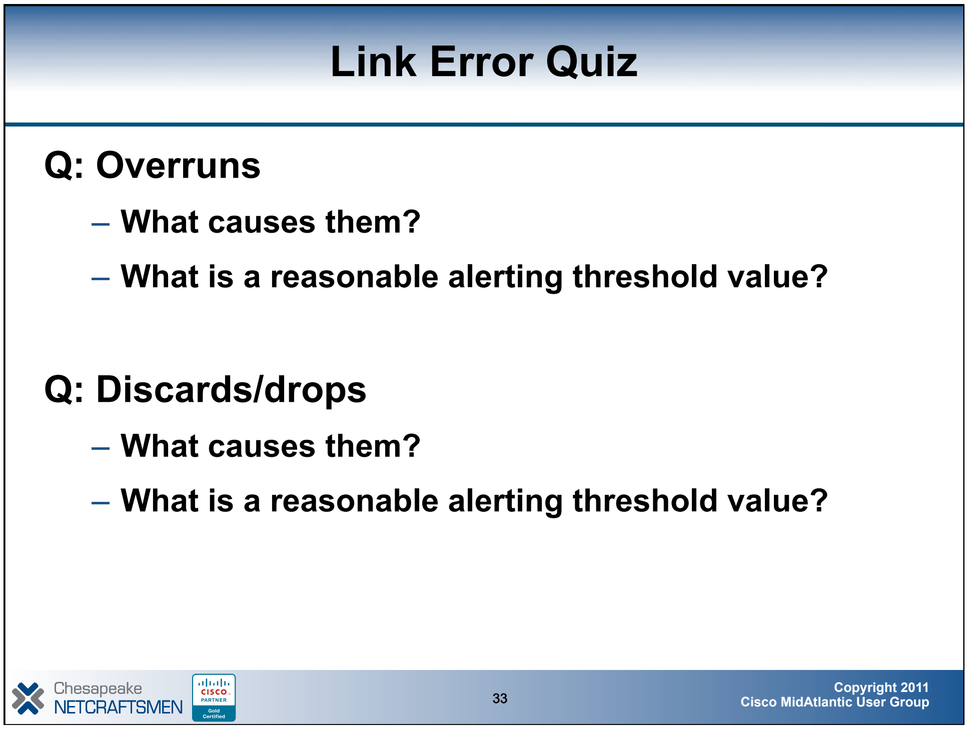
95th Percentile Example Dataset

- Utilization: 1.32Mbps max and 0.27Mbps avg



95th Percentile Sorted Dataset

- 95th Percentile utilization: 0.75Mbps



Link Error Quiz

Q: Overruns

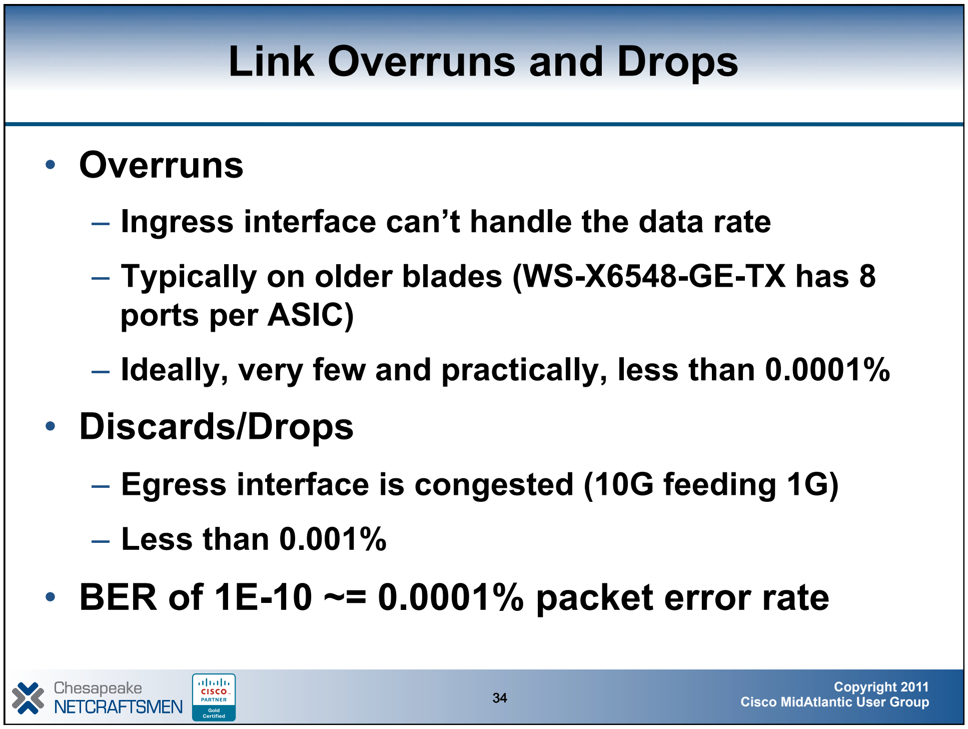
- What causes them?
- What is a reasonable alerting threshold value?

Q: Discards/drops

- What causes them?
- What is a reasonable alerting threshold value?

33

Copyright 2011
Cisco MidAtlantic User Group

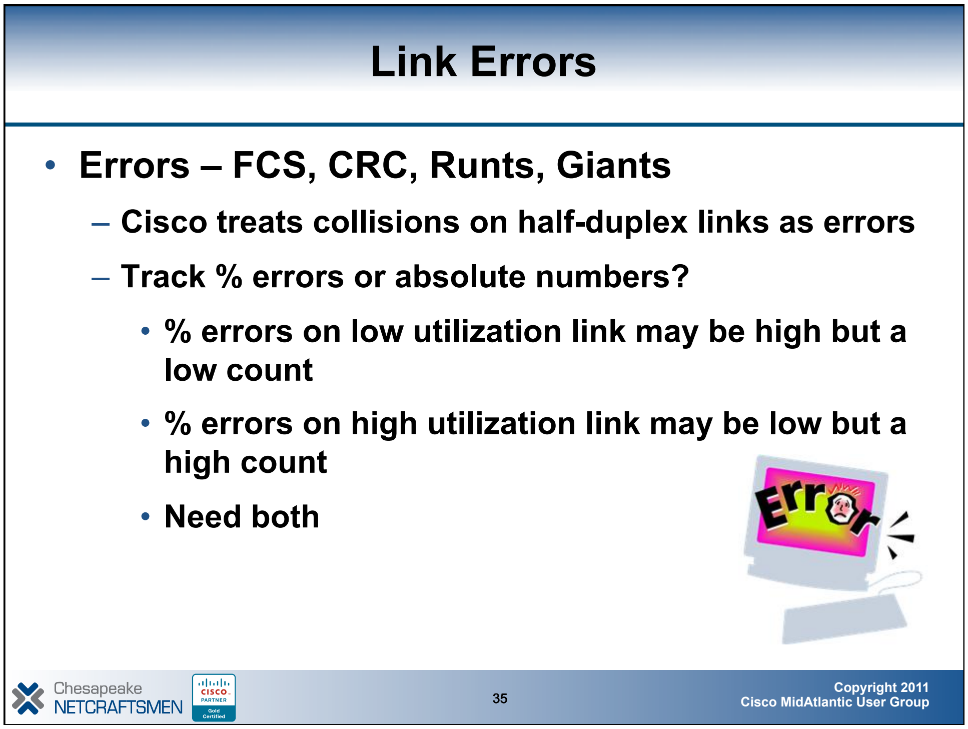


Link Overruns and Drops

- Overruns
  - Ingress interface can’t handle the data rate
  - Typically on older blades (WS-X6548-GE-TX has 8 ports per ASIC)
  - Ideally, very few and practically, less than 0.0001%
- Discards/Drops
  - Egress interface is congested (10G feeding 1G)
  - Less than 0.001%
- BER of 1E-10 ~= 0.0001% packet error rate

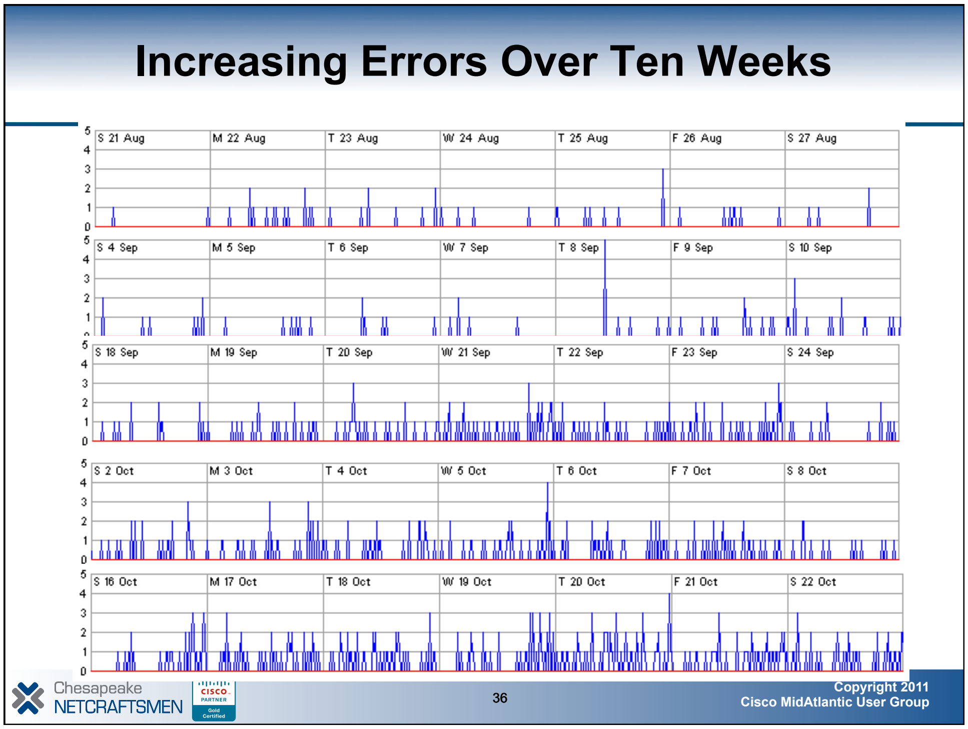
34

Copyright 2011
Cisco MidAtlantic User Group

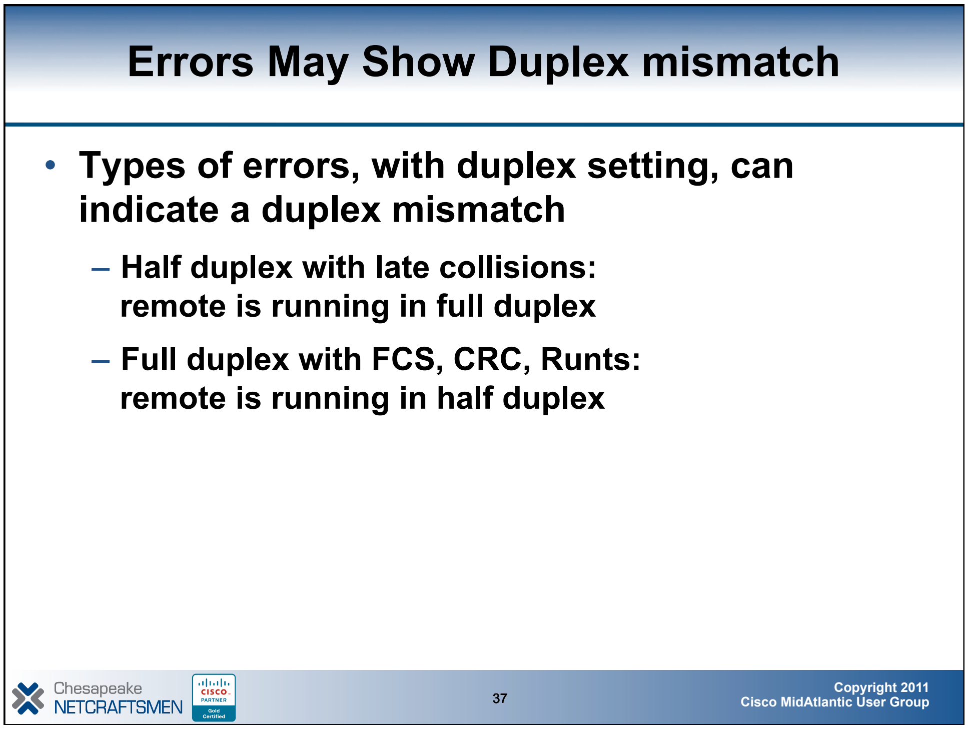


Link Errors

- Errors – FCS, CRC, Runts, Giants
  - Cisco treats collisions on half-duplex links as errors
  - Track % errors or absolute numbers?
    - % errors on low utilization link may be high but a low count
    - % errors on high utilization link may be low but a high count
    - Need both



Increasing Errors Over Ten Weeks



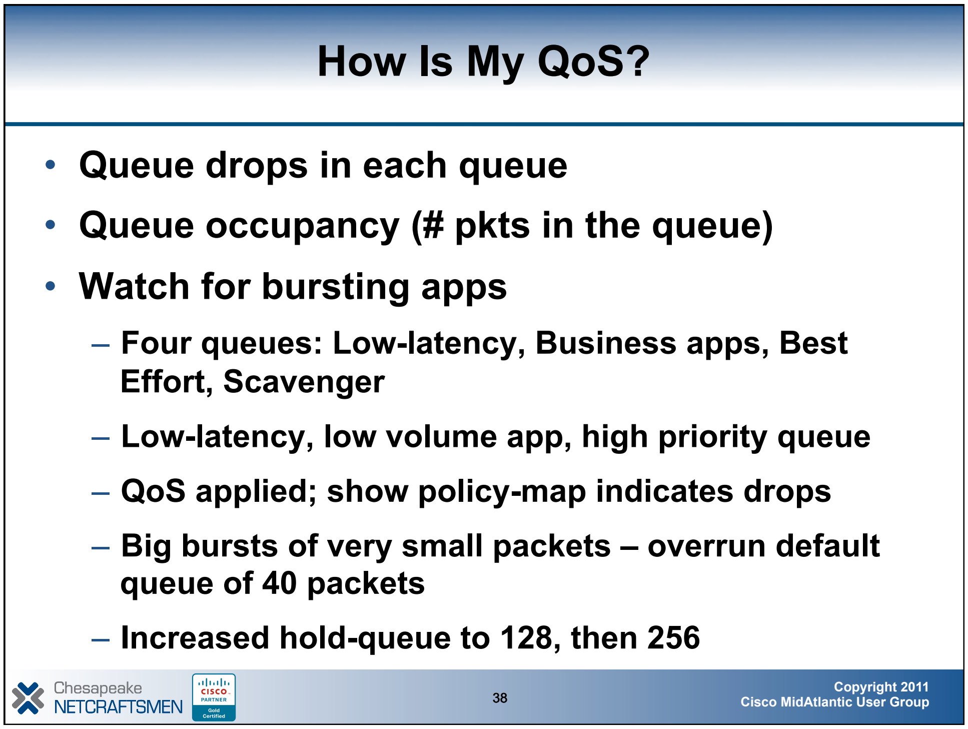
Errors May Show Duplex mismatch

- Types of errors, with duplex setting, can indicate a duplex mismatch
  - Half duplex with late collisions: remote is running in full duplex
  - Full duplex with FCS, CRC, Runts: remote is running in half duplex

Chesapeake NETCRAFTSMEN

37

Copyright 2011
Cisco MidAtlantic User Group



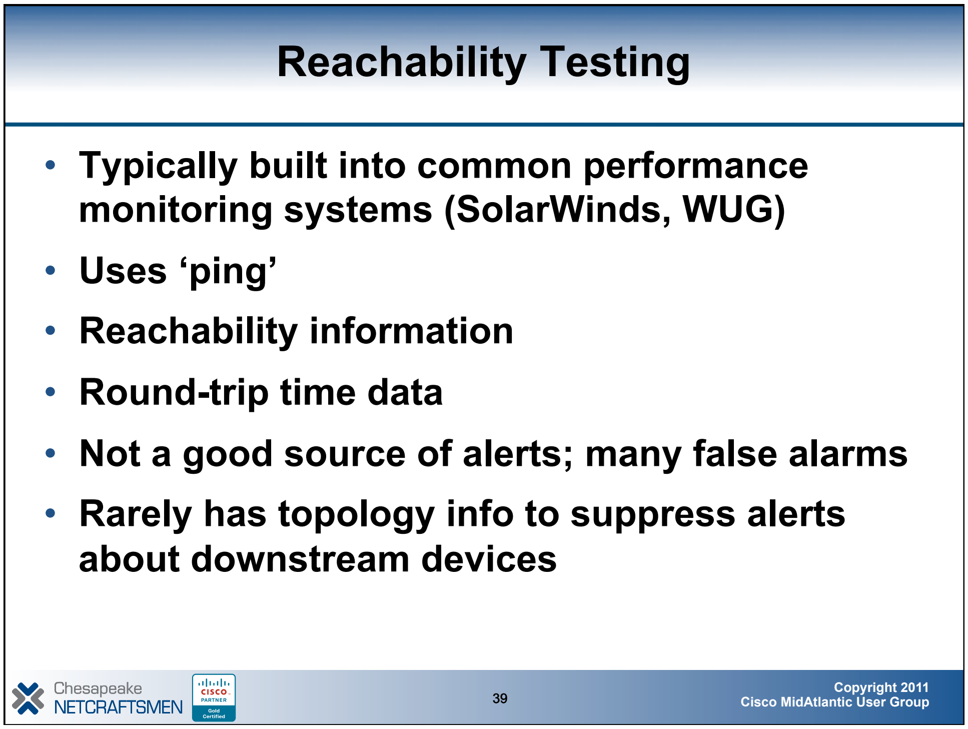
How Is My QoS?

- Queue drops in each queue
- Queue occupancy (# pkts in the queue)
- Watch for bursting apps
  - Four queues: Low-latency, Business apps, Best Effort, Scavenger
  - Low-latency, low volume app, high priority queue
  - QoS applied; show policy-map indicates drops
  - Big bursts of very small packets – overrun default queue of 40 packets
  - Increased hold-queue to 128, then 256

Chesapeake NETCRAFTSMEN

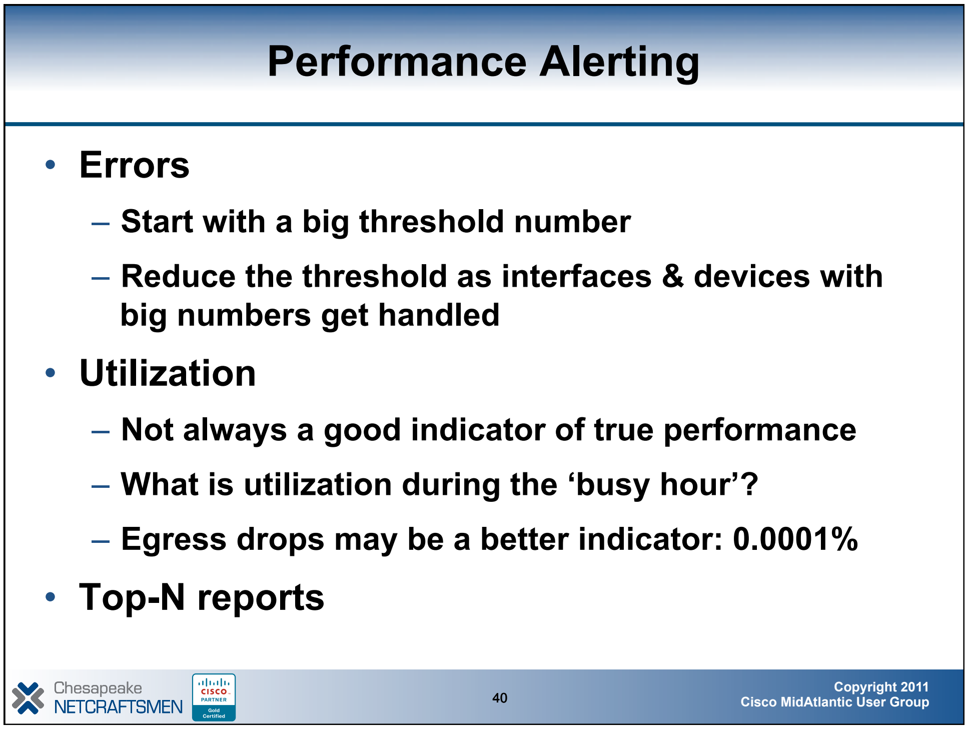
38

Copyright 2011
Cisco MidAtlantic User Group



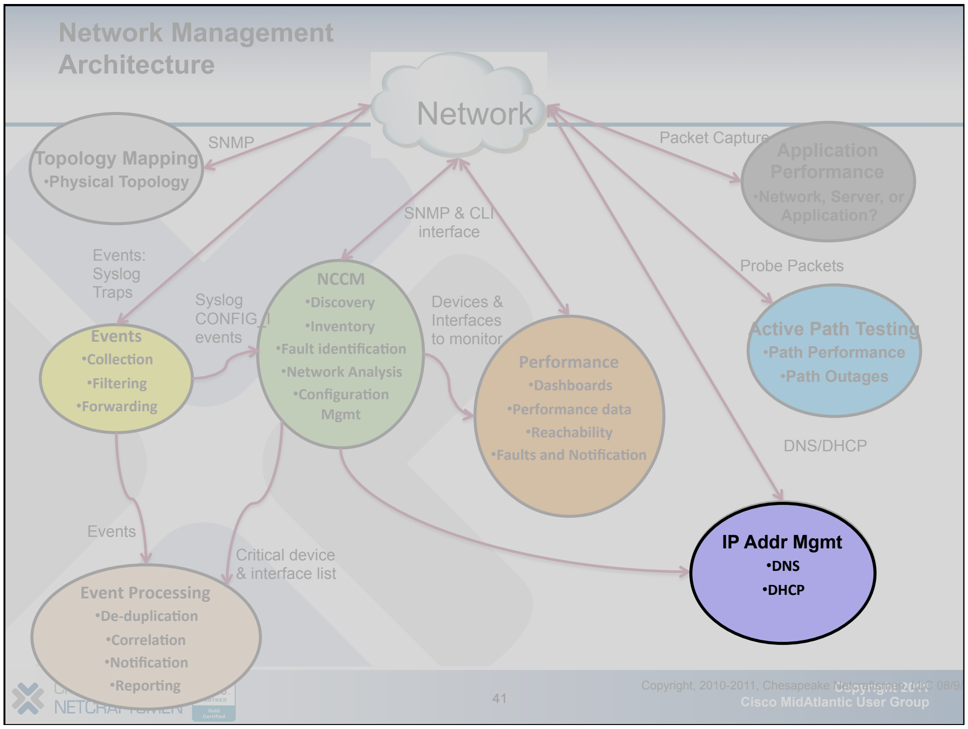
Reachability Testing

- Typically built into common performance monitoring systems (SolarWinds, WUG)
- Uses ‘ping’
- Reachability information
- Round-trip time data
- Not a good source of alerts; many false alarms
- Rarely has topology info to suppress alerts about downstream devices



Performance Alerting

- Errors
  - Start with a big threshold number
  - Reduce the threshold as interfaces & devices with big numbers get handled
- Utilization
  - Not always a good indicator of true performance
  - What is utilization during the ‘busy hour’?
  - Egress drops may be a better indicator: 0.0001%
- Top-N reports



Network Management Architecture

Network

SNMP

Topology Mapping
- Physical Topology

Packet Capture

Application Performance
- Network, Server, or Application?

SNMP & CLI interface

Events: Syslog Traps

Syslog CONFIG_I events

Probe Packets

NCCM
- Discovery
- Inventory
- Fault identification
- Network Analysis
- Configuration Mgmt

Devices & Interfaces to monitor

Events
- Collection
- Filtering
- Forwarding

Active Path Testing
- Path Performance
- Path Outages

Performance
- Dashboards
- Performance data
- Reachability
- Faults and Notification

DNS/DHCP

Events

Critical device & interface list

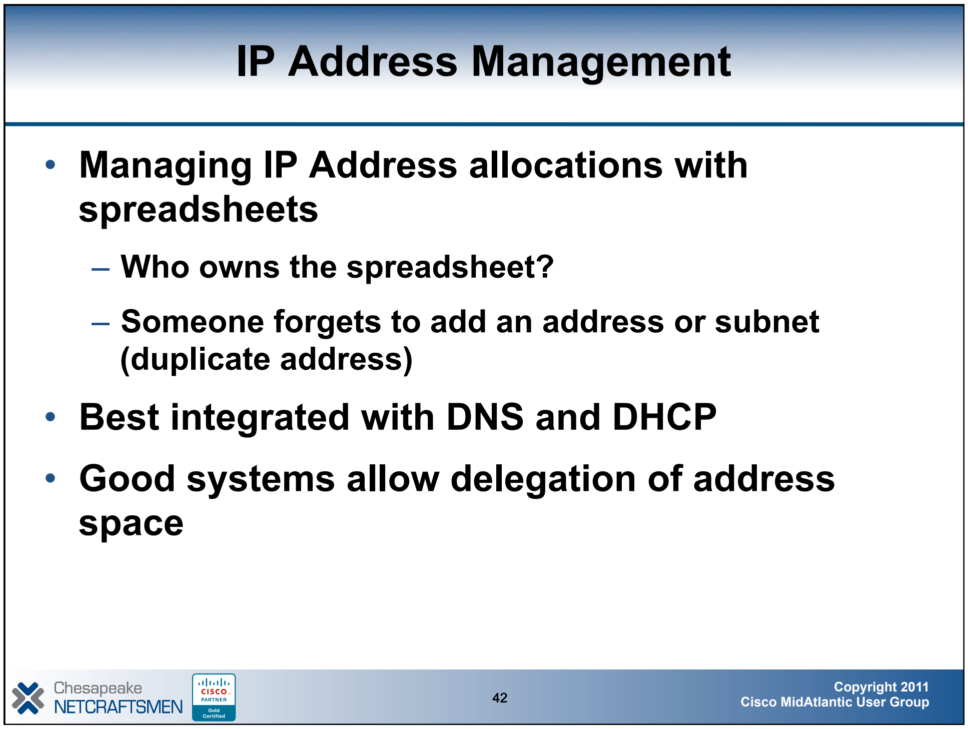
IP Addr Mgmt
- DNS
- DHCP

Event Processing
- De-duplication
- Correlation
- Notification
- Reporting

41

Copyright, 2010-2011, Chesapeake NetCraftsmen, LLC 08/

Copyright 2011
Cisco MidAtlantic User Group

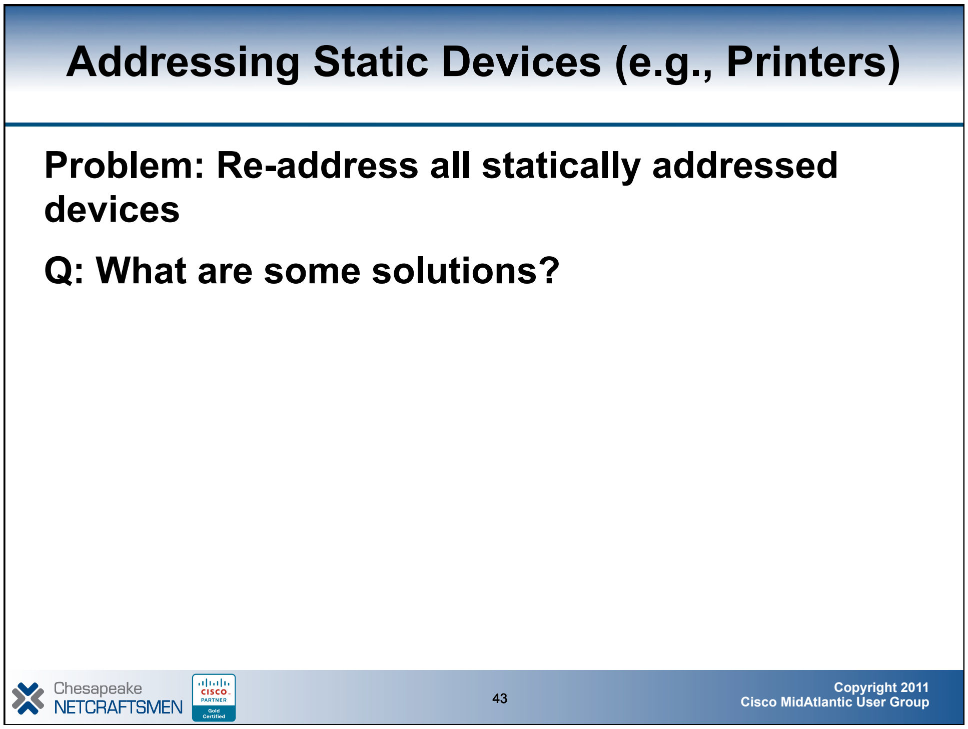


IP Address Management

- Managing IP Address allocations with spreadsheets
  - Who owns the spreadsheet?
  - Someone forgets to add an address or subnet (duplicate address)
- Best integrated with DNS and DHCP
- Good systems allow delegation of address space

42

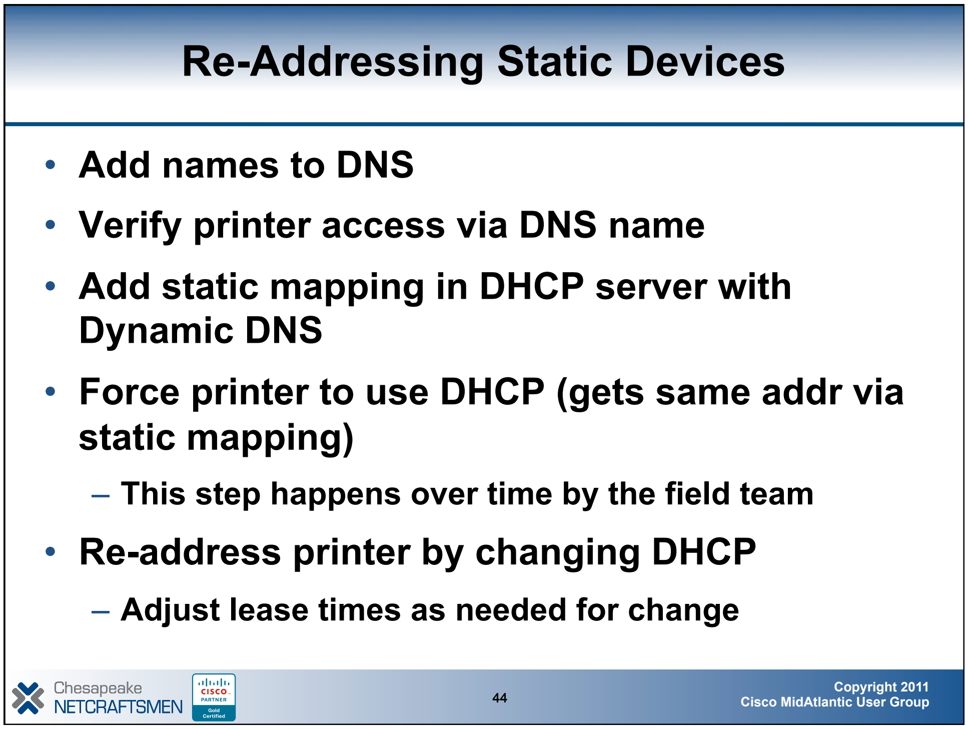
Copyright 2011
Cisco MidAtlantic User Group



Addressing Static Devices (e.g., Printers)

Problem: Re-address all statically addressed devices

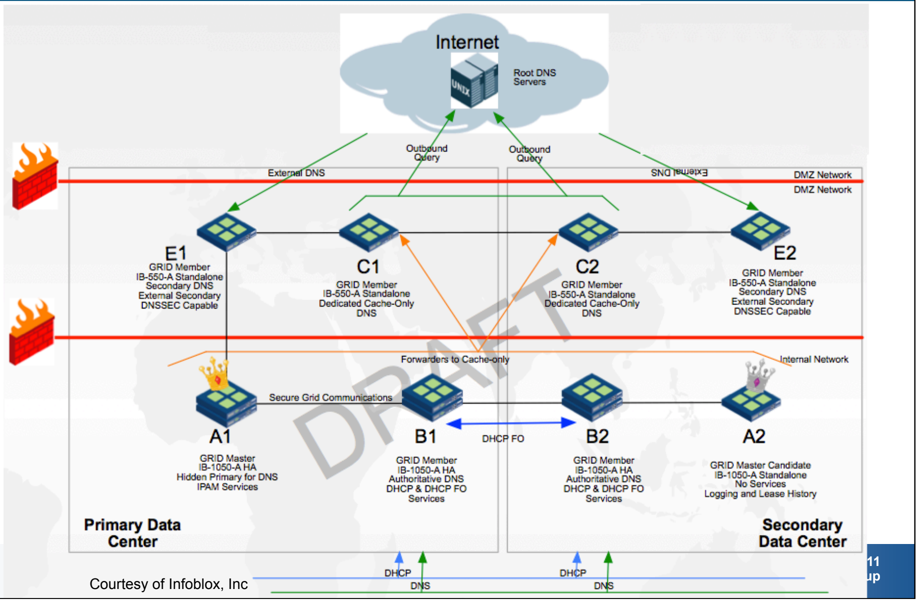
Q: What are some solutions?



Re-Addressing Static Devices

- Add names to DNS
- Verify printer access via DNS name
- Add static mapping in DHCP server with Dynamic DNS
- Force printer to use DHCP (gets same addr via static mapping)
  - This step happens over time by the field team
- Re-address printer by changing DHCP
  - Adjust lease times as needed for change

DNS/DHCP/IPAM Architecture



Courtesy of Infoblox, Inc

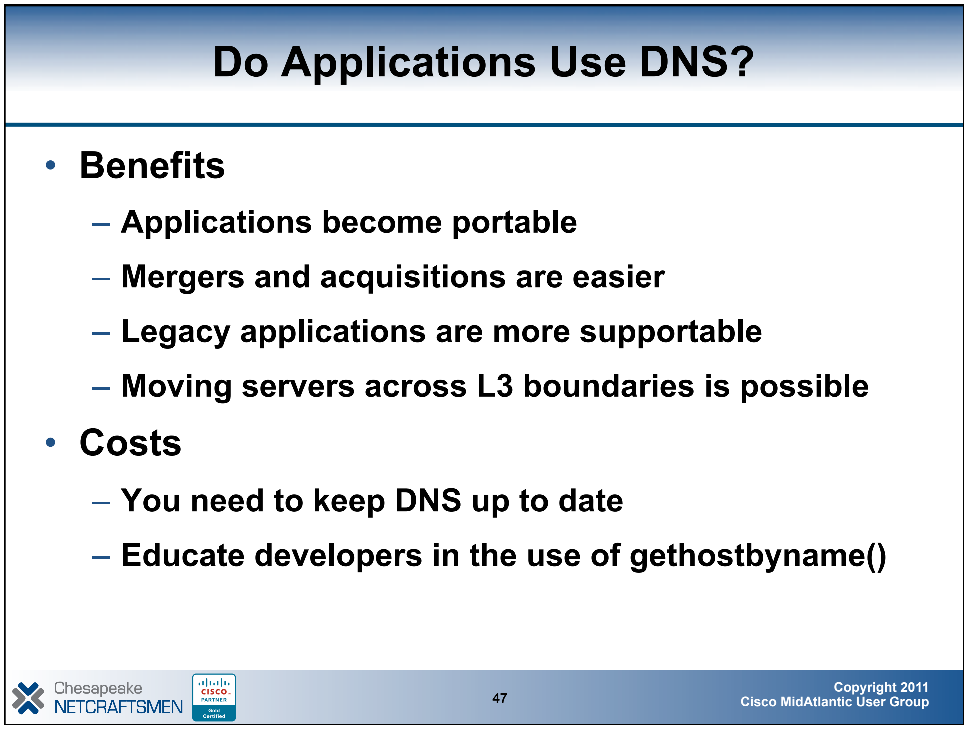
Device Naming Conventions

Field Names	Site	Location	Function	Unit
Field Lengths	2-3	Variable	3-4	1-2
Examples	HQ	3rd floor (3fl)	Access switch (acc)	1

- **Examples**

```
hq-3fl-asw-1 or hq3flasw1
bos-25st-acc1 or bos25-acc1
wdc-14st8fl-dis1 or wdc14st8-dis1
```

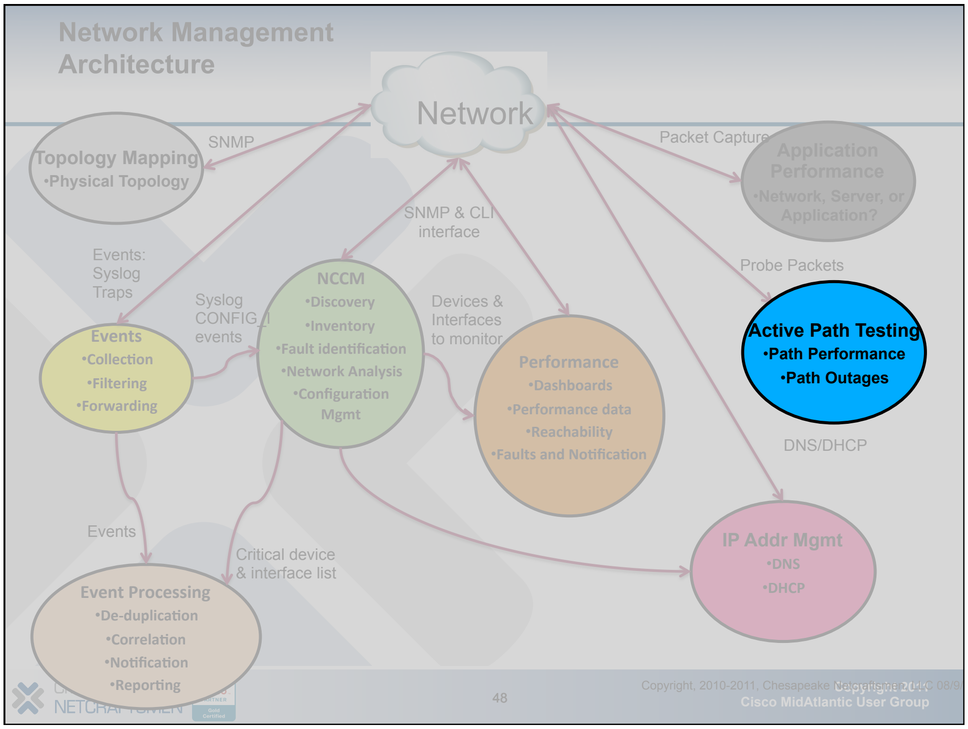
- **Be consistent; aids in troubleshooting & docs**



Do Applications Use DNS?

- **Benefits**
  - Applications become portable
  - Mergers and acquisitions are easier
  - Legacy applications are more supportable
  - Moving servers across L3 boundaries is possible
- **Costs**
  - You need to keep DNS up to date
  - Educate developers in the use of gethostbyname()

Chesapeake NETCRAFTSMEN 47 Copyright 2011 Cisco MidAtlantic User Group



Network Management Architecture

Network

SNMP

Topology Mapping
•Physical Topology

Packet Capture

Application Performance
•Network, Server, or Application?

SNMP & CLI interface

Events: Syslog Traps

Syslog CONFIG_I events

NCCM
•Discovery
•Inventory
•Fault identification
•Network Analysis
•Configuration Mgmt

Devices & Interfaces to monitor

Probe Packets

Active Path Testing
•Path Performance
•Path Outages

Events
•Collection
•Filtering
•Forwarding

Performance
•Dashboards
•Performance data
•Reachability
•Faults and Notification

DNS/DHCP

Events

Critical device & interface list

IP Addr Mgmt
•DNS
•DHCP

Event Processing
•De-duplication
•Correlation
•Notification
•Reporting

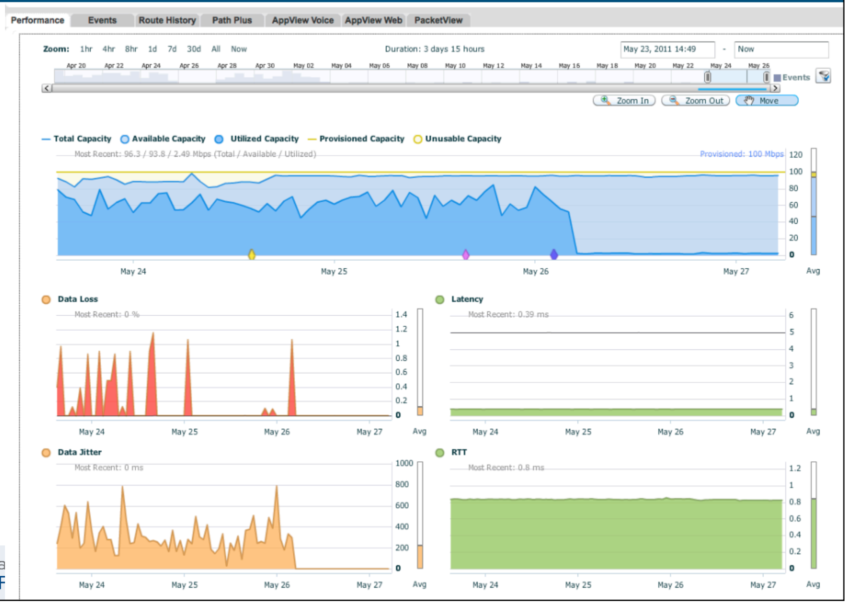
Copyright, 2010-2011, Chesapeake NetCraftsmen

48 Copyright 2011 Cisco MidAtlantic User Group

Active Path Testing

- More Detailed than ‘ping’ tests
- Device and interface monitoring isn’t enough
  - C6500 blade inserted; wedged forwarding plane; control plane running => black hole path
- What is the path available capacity?
- Delay, jitter, and packet loss?
- How do you know when the stats change?
- Alerts when thresholds are exceeded

Path Test Results



Duration: 3 days 15 hours

May 23, 2011 14:49 - Now

Most Recent: 96.3 / 93.8 / 2.49 Mbps (Total / Available / Utilized)

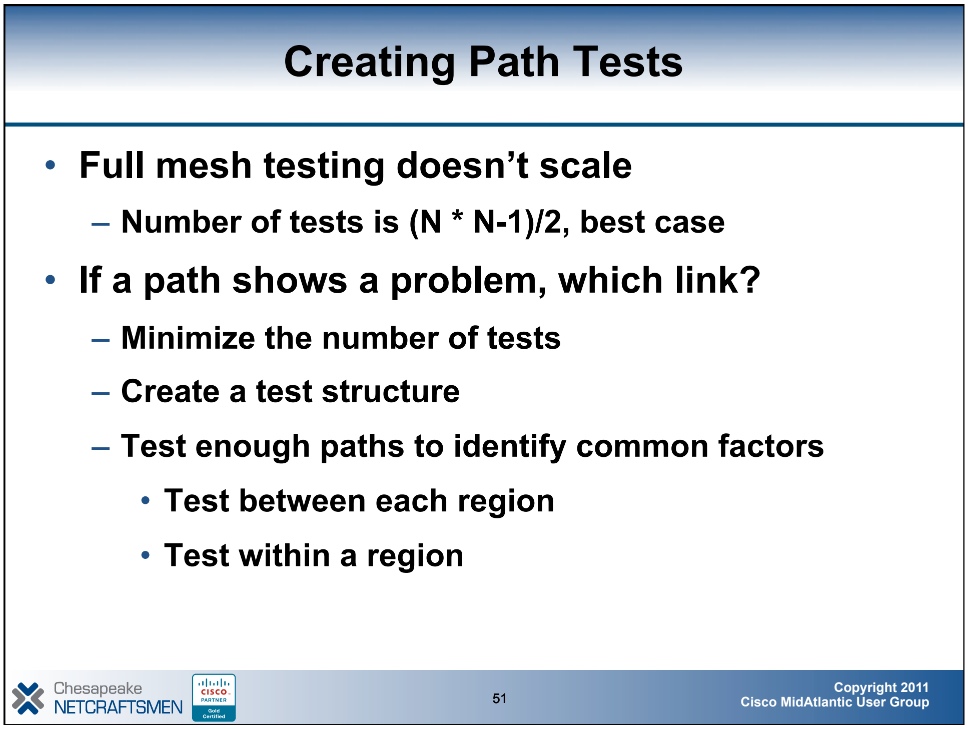
Provisioned: 100 Mbps

Data Loss: Most Recent: 0 %

Latency: Most Recent: 0.39 ms

Data Jitter: Most Recent: 0 ms

RTT: Most Recent: 0.8 ms



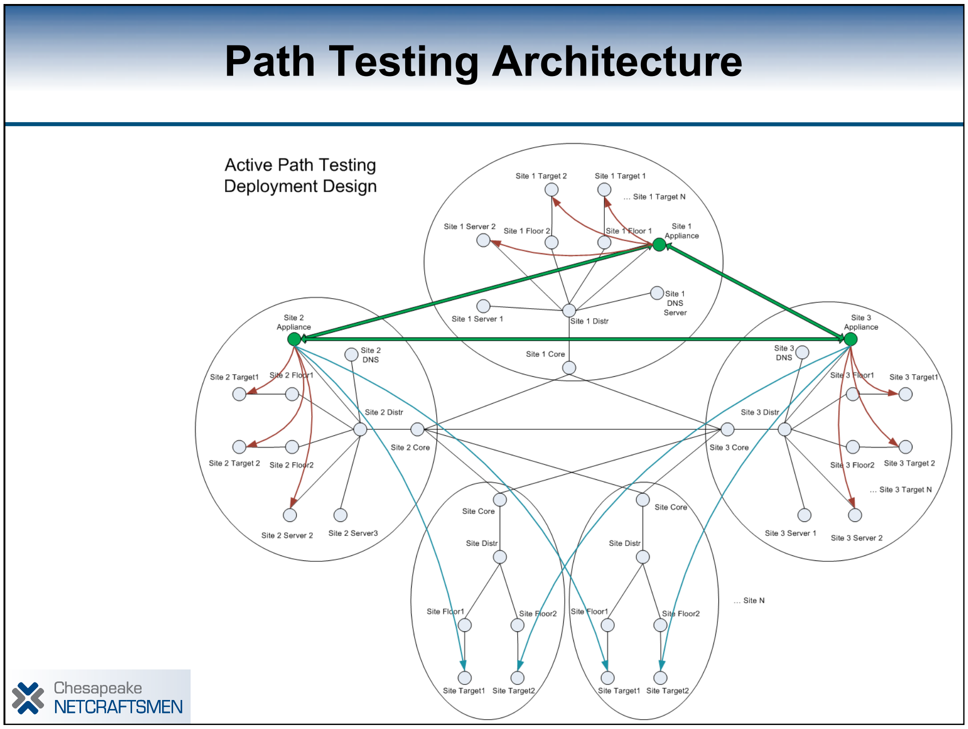
Creating Path Tests

- Full mesh testing doesn't scale
  - Number of tests is (N * N-1)/2, best case
- If a path shows a problem, which link?
  - Minimize the number of tests
  - Create a test structure
  - Test enough paths to identify common factors
    - Test between each region
    - Test within a region

Chesapeake NETCRAFTSMEN

51

Copyright 2011
Cisco MidAtlantic User Group

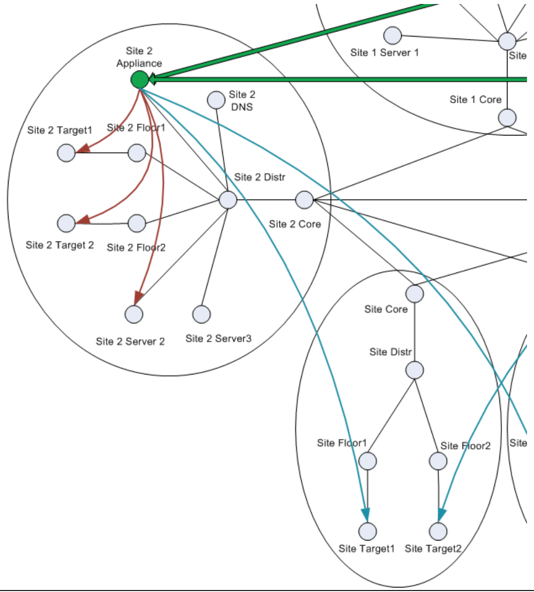


Path Testing Architecture

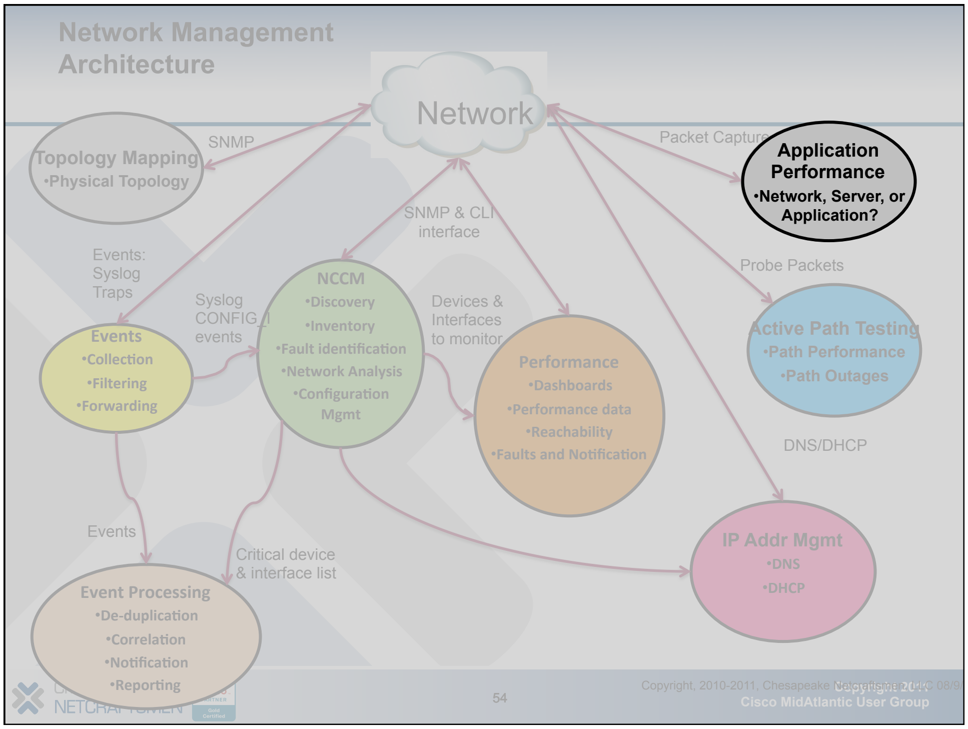
Active Path Testing
Deployment Design

Chesapeake NETCRAFTSMEN

Regional Path Testing



Chesapeake NETCRAFTSMEN



Network Management Architecture

Network

SNMP

Topology Mapping
- Physical Topology

Packet Capture

Application Performance
- Network, Server, or Application?

SNMP & CLI interface

Events: Syslog Traps

Probe Packets

NCCM
- Discovery
- Inventory
- Fault identification
- Network Analysis
- Configuration Mgmt

Syslog CONFIG_I events

Devices & Interfaces to monitor

Active Path Testing
- Path Performance
- Path Outages

Events
- Collection
- Filtering
- Forwarding

Performance
- Dashboards
- Performance data
- Reachability
- Faults and Notification

DNS/DHCP

Events

Critical device & interface list

IP Addr Mgmt
- DNS
- DHCP

Event Processing
- De-duplication
- Correlation
- Notification
- Reporting

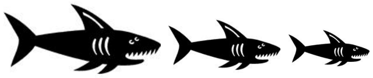
54

Copyright, 2010-2011, Chesapeake NetCraftsmen, LLC 08/

Cisco MidAtlantic User Group

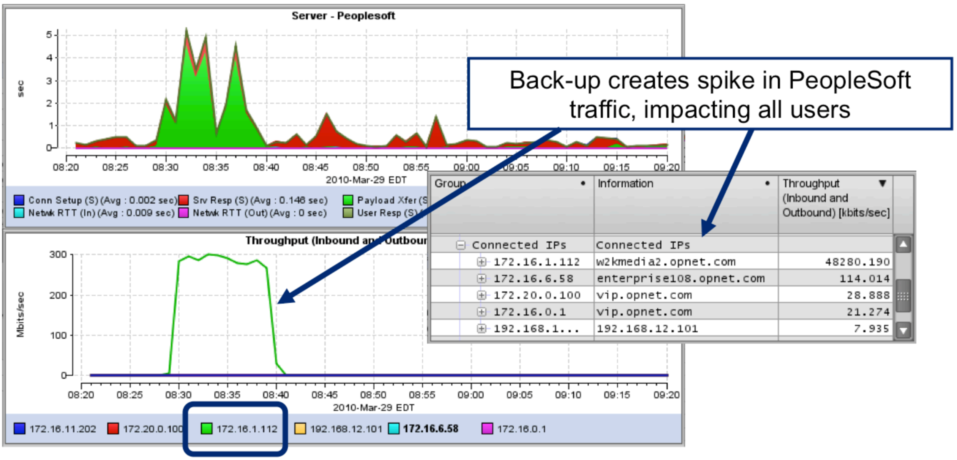
Application Performance

- Based on packet capture & analysis
  - Which devices are communicating?
  - What protocols are being used?
  - How much bandwidth is consumed?
  - Is there significant packet loss?
  - What is the server response time?
  - What is the network latency?
- Can be done with wireshark, but is tedious



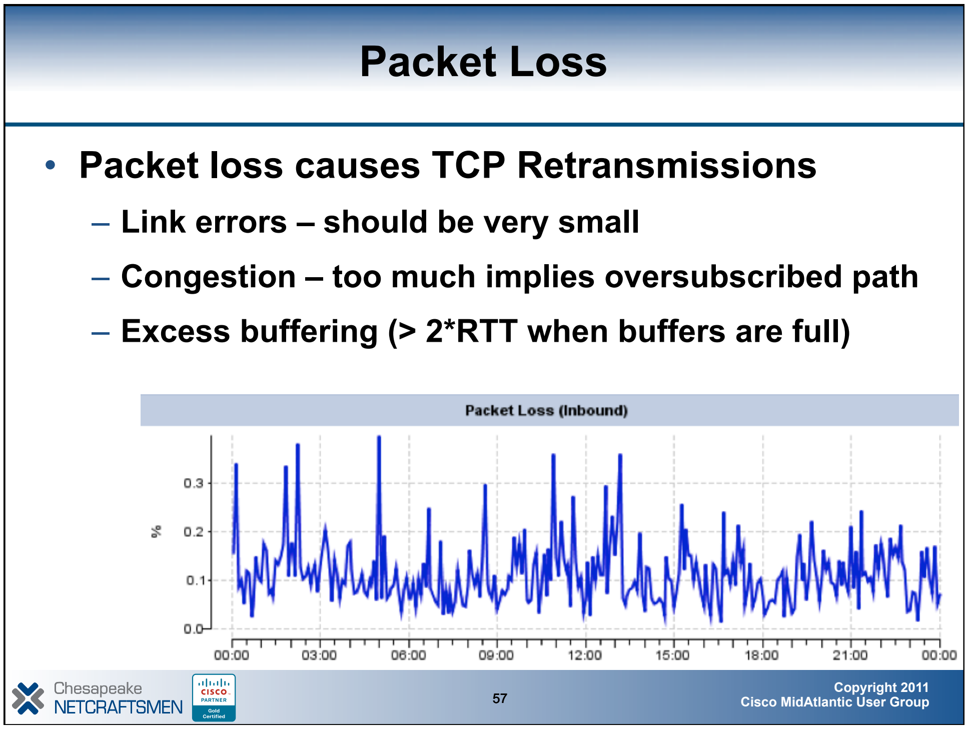
Bandwidth Hogs

- T3 link with 50% “entertainment traffic” (pandora, akamai, limelight)



Back-up creates spike in PeopleSoft traffic, impacting all users

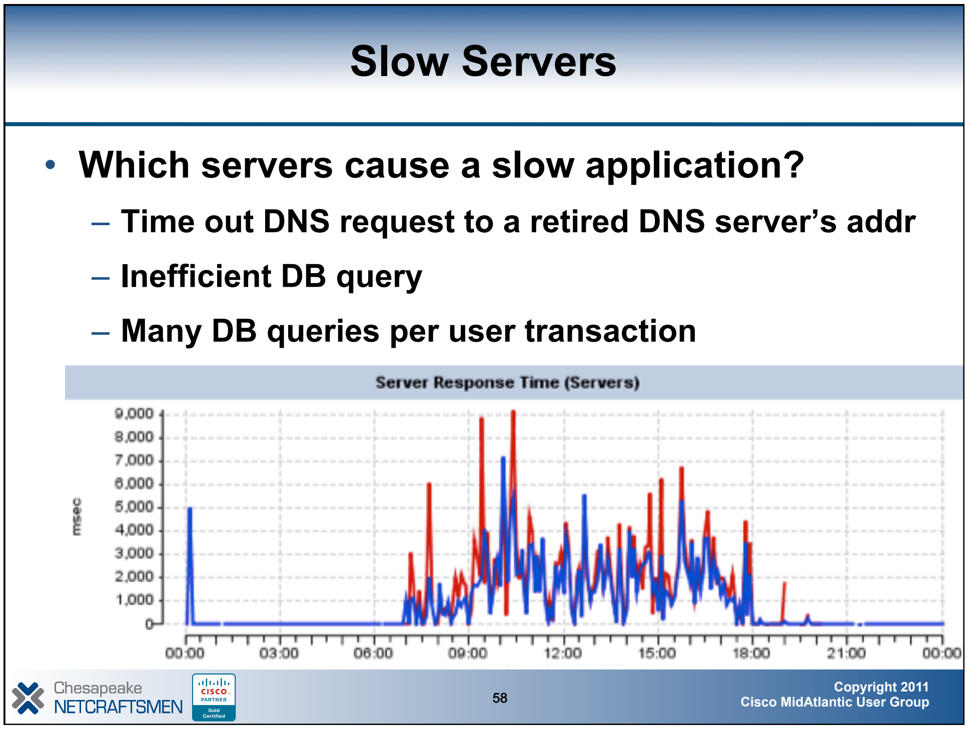
Group	Information	Throughput (Inbound and Outbound) [kbits/sec]
⊟ Connected IPs	Connected IPs	
⊞ 172.16.1.112	w2kmedia2.opnet.com	48280.190
⊞ 172.16.6.58	enterprise108.opnet.com	114.014
⊞ 172.20.0.100	vip.opnet.com	28.888
⊞ 172.16.0.1	vip.opnet.com	21.274
⊞ 192.168.1...	192.168.12.101	7.935



Packet Loss

- Packet loss causes TCP Retransmissions
  - Link errors – should be very small
  - Congestion – too much implies oversubscribed path
  - Excess buffering (> 2*RTT when buffers are full)

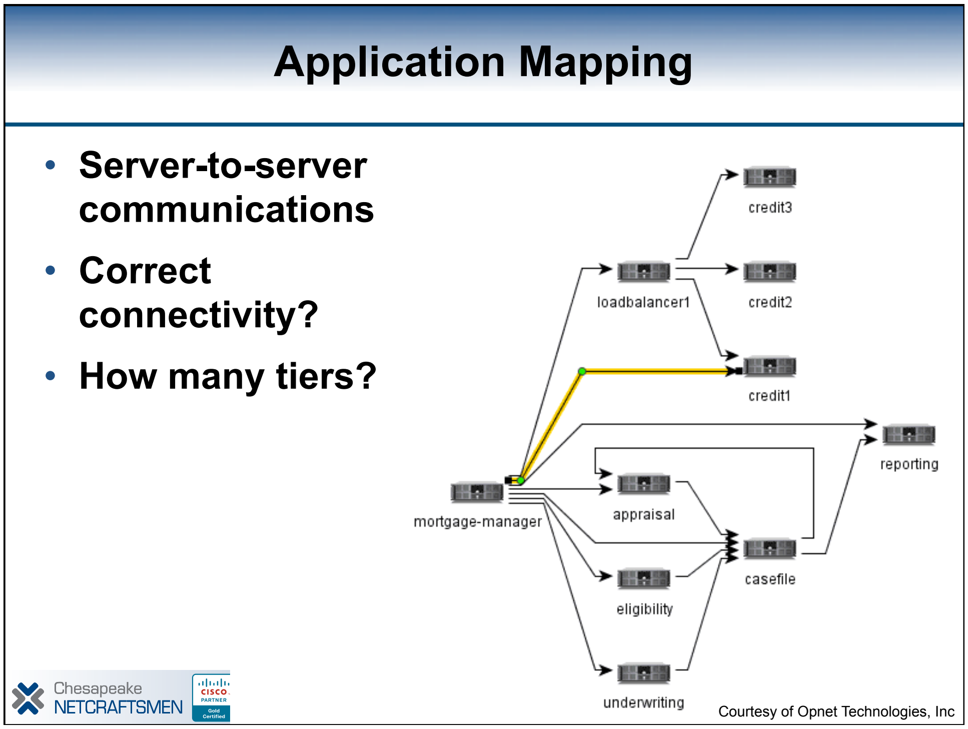
Chesapeake NETCRAFTSMEN 57 Copyright 2011 Cisco MidAtlantic User Group



Slow Servers

- Which servers cause a slow application?
  - Time out DNS request to a retired DNS server's addr
  - Inefficient DB query
  - Many DB queries per user transaction

Chesapeake NETCRAFTSMEN 58 Copyright 2011 Cisco MidAtlantic User Group

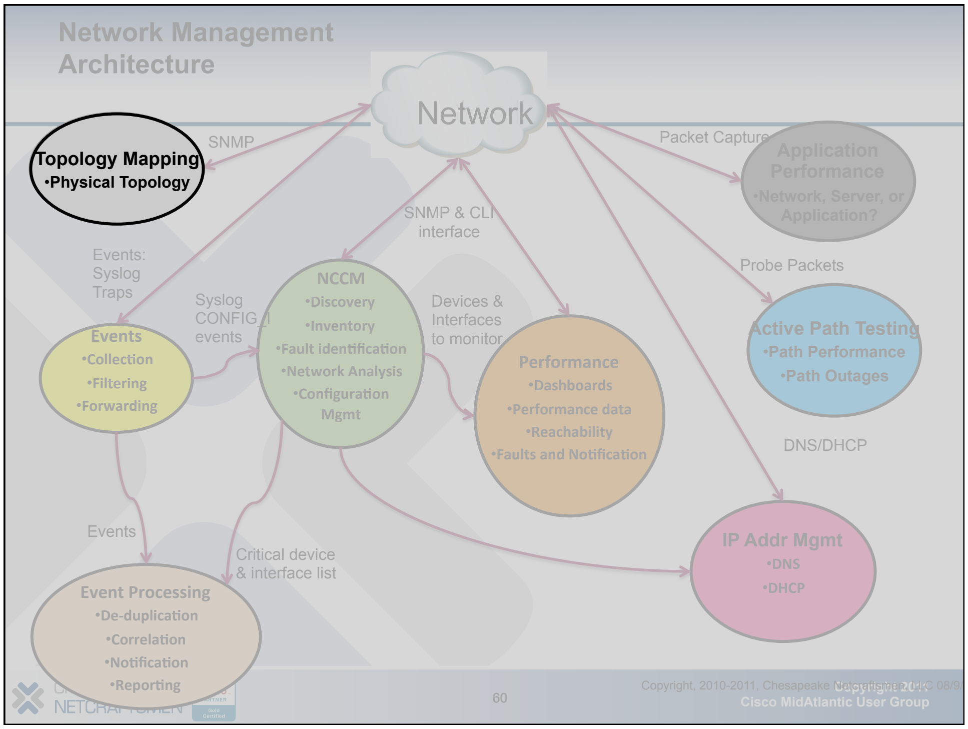


Application Mapping

- Server-to-server communications
- Correct connectivity?
- How many tiers?

Courtesy of Opnet Technologies, Inc

Chesapeake NETCRAFTSMEN



Network Management Architecture

Network

Topology Mapping
•Physical Topology

SNMP

Packet Capture

Application Performance
•Network, Server, or Application?

SNMP & CLI interface

Events:
Syslog
Traps

Probe Packets

Syslog
CONFIG_I
events

NCCM
•Discovery
•Inventory
•Fault identification
•Network Analysis
•Configuration Mgmt

Devices & Interfaces to monitor

Events
•Collection
•Filtering
•Forwarding

Performance
•Dashboards
•Performance data
•Reachability
•Faults and Notification

Active Path Testing
•Path Performance
•Path Outages

DNS/DHCP

Events

Critical device & interface list

IP Addr Mgmt
•DNS
•DHCP

Event Processing
•De-duplication
•Correlation
•Notification
•Reporting

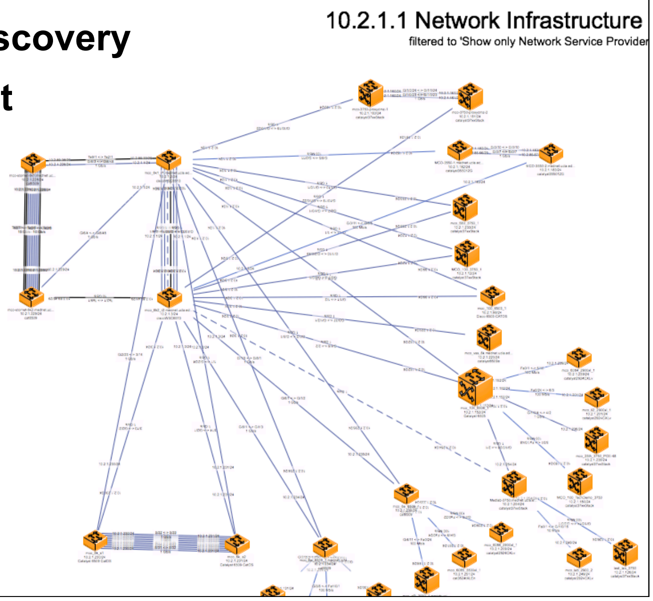
60

Copyright, 2010-2011, Chesapeake Netcraftsmen, LLC 08/9/

Copyright 2011
Cisco MidAtlantic User Group

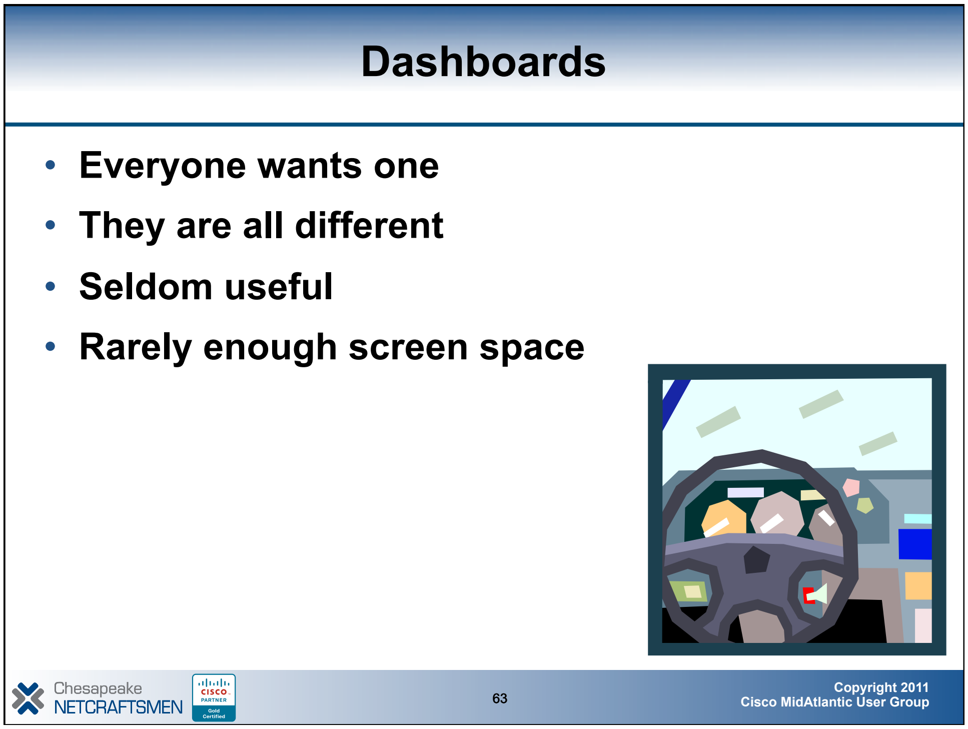
Topology Mapping

- Automatic discovery
- Manual layout


10.2.1.1 Network Infrastructure
filtered to 'Show only Network Service Provider

Topology Mapping

- Typically layer 1 (physical topology)
- Divide the network into core + regions
- Automatic regeneration is a big win
  - Re-use the prior topology layout
  - Show devices newly discovered and newly deleted



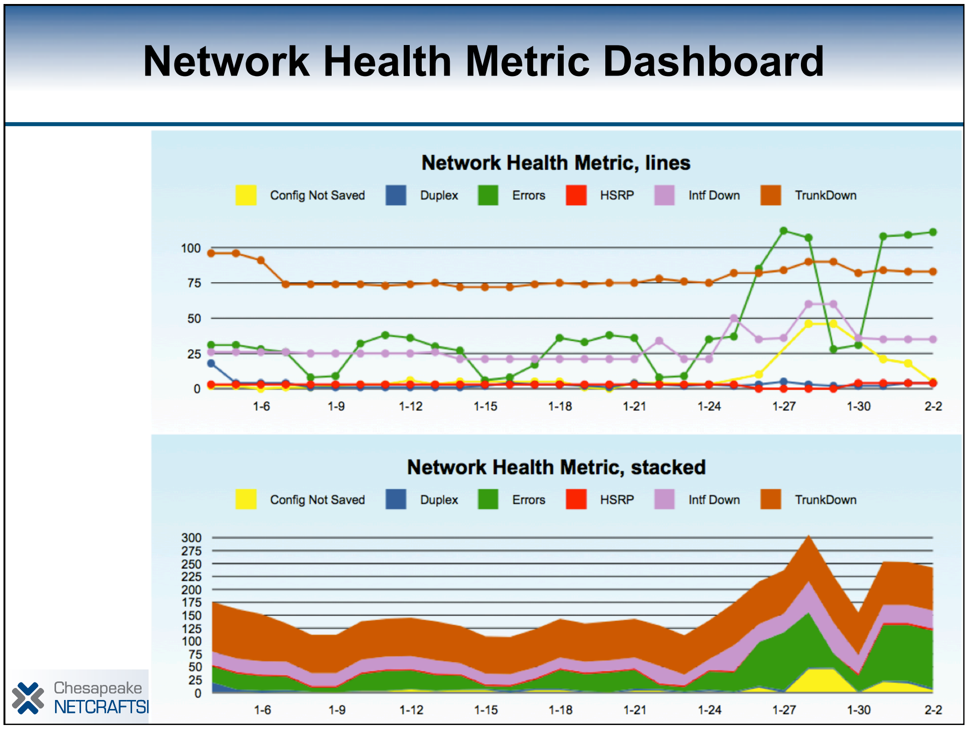
Dashboards

- Everyone wants one
- They are all different
- Seldom useful
- Rarely enough screen space

Chesapeake NETCRAFTSMEN

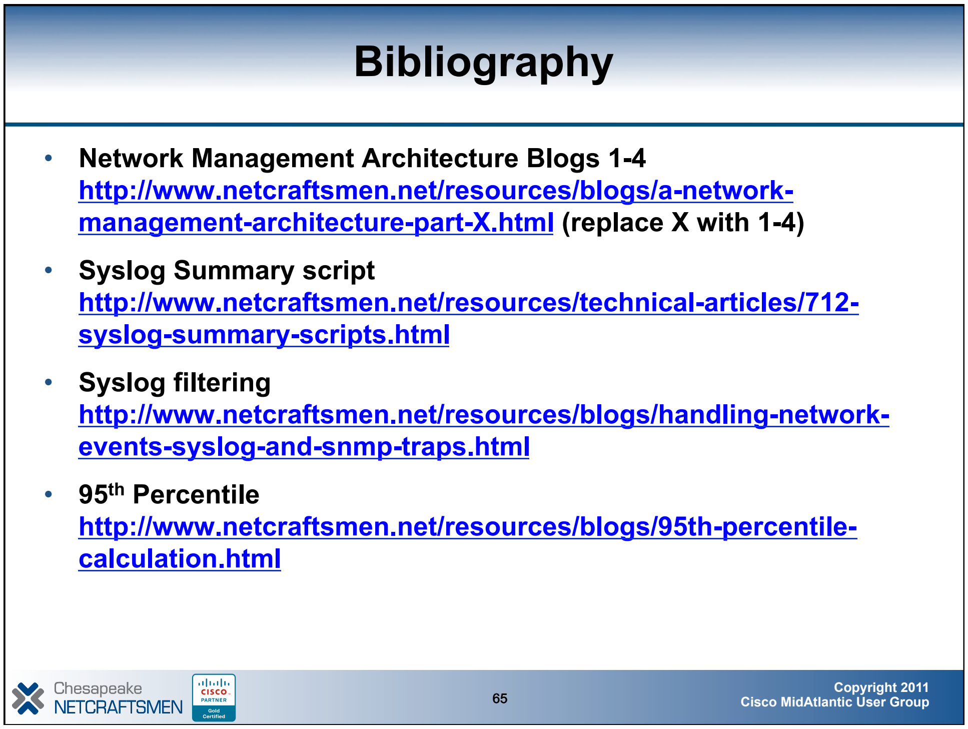
63

Copyright 2011
Cisco MidAtlantic User Group



Network Health Metric Dashboard

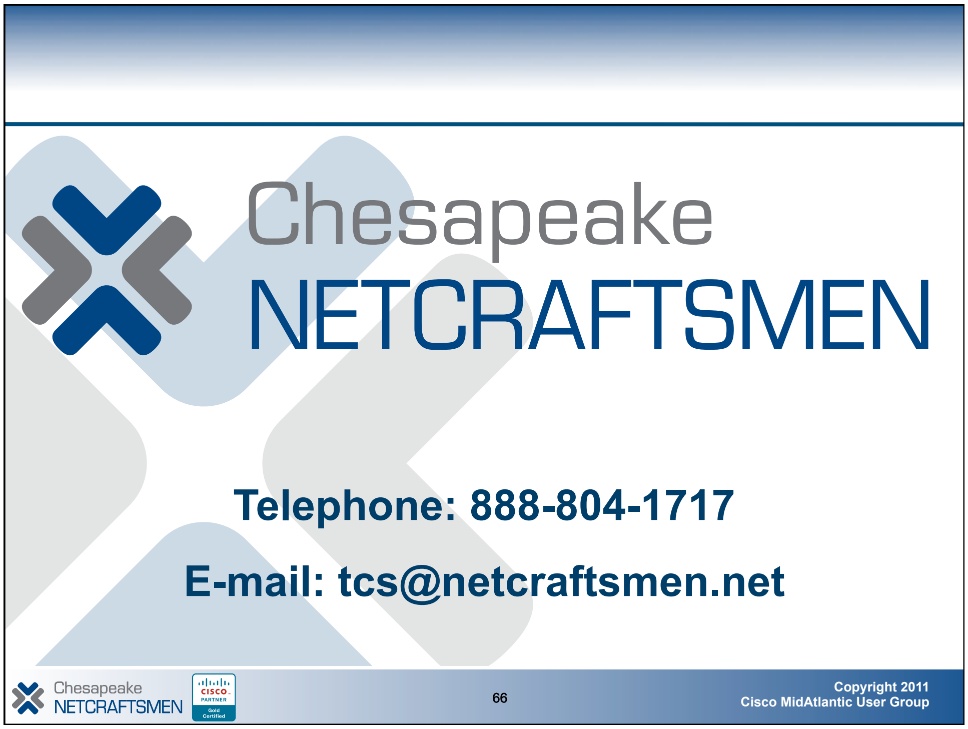
Chesapeake NETCRAFTS



Bibliography

- Network Management Architecture Blogs 1-4
  http://www.netcraftsmen.net/resources/blogs/a-network-management-architecture-part-X.html (replace X with 1-4)
- Syslog Summary script
  http://www.netcraftsmen.net/resources/technical-articles/712-syslog-summary-scripts.html
- Syslog filtering
  http://www.netcraftsmen.net/resources/blogs/handling-network-events-syslog-and-snmp-traps.html
- 95th Percentile
  http://www.netcraftsmen.net/resources/blogs/95th-percentile-calculation.html

Chesapeake NETCRAFTSMEN 65 Copyright 2011 Cisco MidAtlantic User Group



Chesapeake NETCRAFTSMEN

Telephone: 888-804-1717

E-mail: tcs@netcraftsmen.net

Chesapeake NETCRAFTSMEN 66 Copyright 2011 Cisco MidAtlantic User Group