IT3010

Network Design and Management

Lecture 05

Network Monitoring

Shashika Lokuliyana

Faculty of Computing

Department of CSE

SLIIT

Discover Your Future

Network Design and Management

Network Monitoring

Lectuer 5

Today's lecture overview

- Definition of Network Monitoring
- Active vs. Passive monitoring
- Categories for monitoring
  - Network specifications: *Ethernet*
  - Network traffic and protocols
  - Platforms and operating systems (next week lecture)

A definition for Network Monitoring

WIKIPEDIA

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

PCMAG.COM

oring an active communications rk in order to diagnose problems ather statistics for administration and fine tuning.

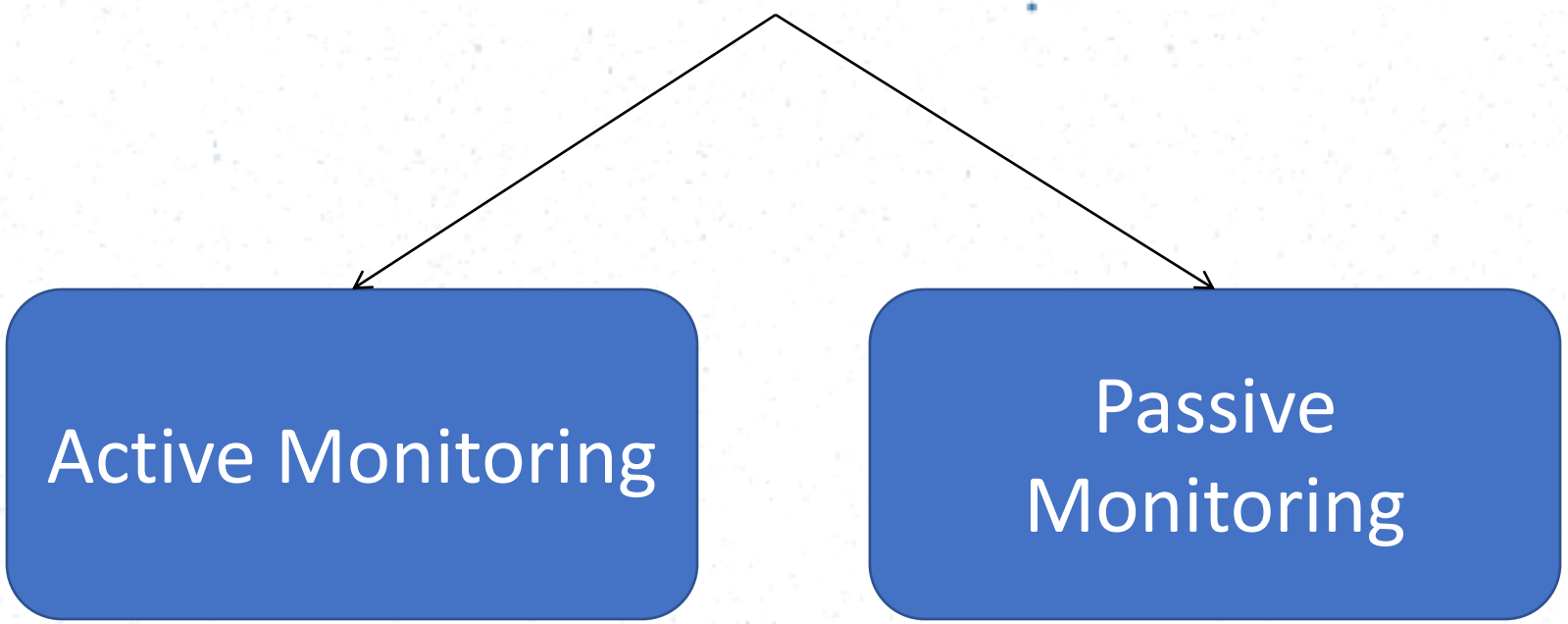
What is Network Monitoring??

- Write it in your terms.

Kevin had a funny feeling that his boss was monitoring his emails

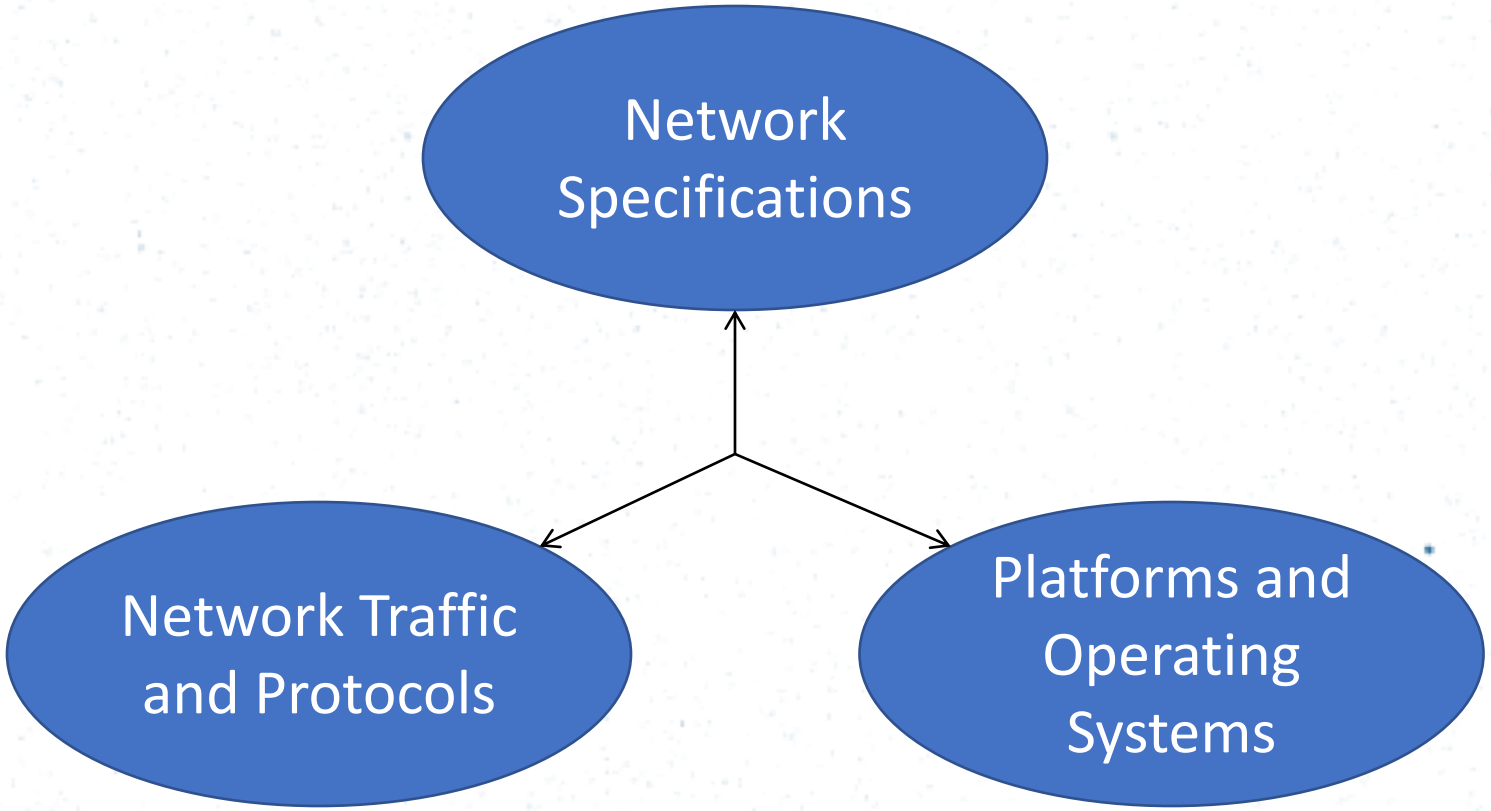
Types of Network Monitoring

Two types of Network Monitoring



Monitoring Categories

Things we will need to monitor…



Monitoring and analysis of Network Specifications

Ethernet

Establishing an Ethernet Baseline

Things to monitor with respect to Ethernet..

- Network utilization
- …
- …
- Collision rate
- Errors

Where it all starts..

```
Router# show interfaces ethernet 0
Ethernet 0 is up, line protocol is up
   Hardware is MCI Ethernet, address is aa00.0400.0134 (via 0000.0c00.4369)
          Internet address is 131.108.1.1, subnet mask is 255.255.255.0
          MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
          Encapsulation ARPA, loopback not set, keepalive set (10 sec)
             ARP type: ARPA, PROBE, ARP Timeout 4:00:00
          Last input 0:00:00, output 0:00:00, output hang never
          Output queue 0/40, 0 drops; input queue 0/75, 2 drops
          Five minute input rate 61000 bits/sec, 4 packets/sec
          Five minute output rate 1000 bits/sec, 2 packets/sec
       2295197 packets input, 305539992 bytes, 0 no buffer
       Received 1925500 broadcasts, 0 runts, 0 giants
       3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
           0 input packets with dribble condition detected
       3594664 packets output, 436549843 bytes, 0 underruns
       8 output errors, 1790 collisions, 10 interface resets, 0 restarts
```

Ethernet Utilization

- Utilization is a network performance measure that specifies the amount of time a LAN spends successfully transmitting data.
- Many performance monitoring tools will provide a user with average and peak utilization times, which are reported as a percentage.

Fact => Delays occur 40% to 50%
Reason => Due to increased collisions
Solution => ……
Expectation => Should achieve 15% to 25%

Peak Utilization

Peak utilization means that, ……

……, a certain percentage of the LAN's capacity was utilized.

- Need to look at
  - ❑ Protocols
  - ❑ Devices
  - ❑ Users
- Determine when peaks occur

Average Utilization

Average utilization means that ……

……(e.g. 10 hours), on average, a certain percentage of the LAN's capacity is used for successfully transmitting data. In simple terms this is the calculated level over longer time.

- What are we averaging?

```
Last input 0:00:00, output 0:00:00, output hang never
Output queue 0/40, 0 drops; input queue 0/75, 2 drops
Five minute input rate 61000 bits/sec, 4 packets/sec
Five minute output rate 1000 bits/sec, 2 packets/sec
2295197 packets input, 305539992 bytes, 0 no buffer
```

- What is bits-per-second?

Current Utilization

Current utilization is the moving average calculated over a small time period (e.g. 5 minutes).

$$\text{new average} = ((\text{average} - \text{interval}) * \exp(-t/C)) + \text{interval}$$

Where:

- t is five seconds, and C is five minutes. exp(−5/(60*5)) == .983. This value is known as the “weighting factor” or “decay factor”.
- newaverage = the value we are trying to compute.
- average = the "newaverage" value calculated from the previous sample.
- interval = the value of the current sample.

Additional Resources for Utilization Monitoring

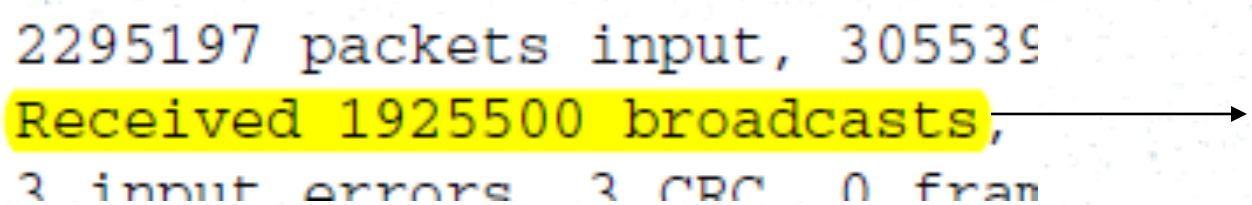
Please make sure to read the following PDF documents uploaded to the course web.

1. Extracted_from_Networking_Explained_Part_1.pdf *(2 pages)*
2. Extracted_from_Networking_Explained_Part_2.pdf *(2 pages)*
3. Understanding_the_bits_per_second.pdf *(3 pages)*

Note

Please note that the first two documents in the above list are two parts of the same document. You should refer starting from Ques #26 in part 1 and continue up to and including Ques #32 in part 2.

Broadcasts



Broadcast
+
Multicast

- Excessive amounts of broadcast or multicast traffic,

- Broadcasts Rate should not exceed 5-10%

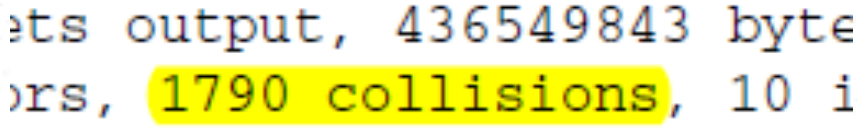
Multicasts

- Communication between small groups of devices.
- Same rules as broadcast.

Examining Ethernet Errors

- Collisions
- Short frames
- Bad FCS
- Long frames
- Ghosts

Collisions



If two frames are transmitted simultaneously by two stations, they overlap in time and the resulting signal is garbled. This event is known as a collision.

- Collisions are normal
- CSMA/CD
- Jam signal

Additional Resources for Collisions

- Please make sure to read chapter, “4.2.2 Carrier Sense Multiple Access Protocols (from Pg 255 to Pg 258)” of Tanenbaum’s book.

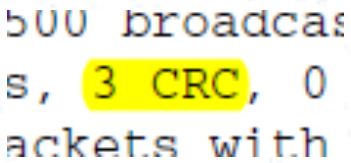
- Please make sure to read the following PDF documents uploaded to the course web.
  1. Causes_for_collisions.pdf *(1 page)*
  2. Troubleshooting_collisions.pdf *(6 pages)*

Short Frames

```
305539992 bytes, 0
asts, 0 runts, 0 gi
0 frame. 0 overrun.
```

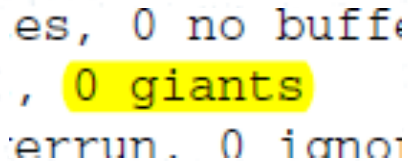
- A short frame is a frame smaller than the minimum legal size of 64 bytes, with a good frame check sequence.
- Caused by,

Bad FCS (Frame Check Sequence)



- A received frame that has a bad Frame Check Sequence, also referred to as a checksum or CRC error, differs from the original transmission by at least one bit.
- In an FCS error frame, the header information is probably correct and the frame may also have a valid size, but the checksum calculated by the receiving station does not match the checksum appended to the end of the frame by the sending station. The frame is then discarded.

Long Frames



- A long frame is a frame larger than the maximum legal size of 1518 bytes.
- It does not consider whether or not the frame had a valid FCS checksum.
- Causes

Ghosts

- Ghosts are classified as energy (noise) detected on the cable that appears to be a frame, but is lacking a valid SFD.
- To qualify as a ghost, the frame must be at least 72 bytes long, including the preamble.
- Slows network, not increased utilization.
- Causes,

Documentation

Ethernet Baseline Statistics			
Network-Based		**Node-Based**	
% Utilization -Peak		% Utilization - Peak	
% Utilization - Average		% Utilization - Average	
Frames/Second - Peak		Frames/Second - Peak	
Frames/Second - Average		Frames/Second - Average	
Frame size - Peak		Frame size - Peak	
Frame size - Average		Frame size - Average	
Total Frame Count		Total Frame Count	
Total Byte Count		Total Byte Count	
Node count - Total		Node/Node Interaction - Total	
Top 10 Nodes		Node/Node Int. - Predominant	
Protocol count - Total		Protocol count - Total	
Protocol count - Top 3		Protocol count - Top 3	
Network Errors		**Station Errors**	
Collisions - Total		Collisions - Total	
Collisions/Second		Collisions/Second	
Runts/Fragments - Total		Runts/Fragments - Total	
Jabbers - Total		Jabbers - Total	
# of CRC/FCS Errors - Total		# of CRC/FCS Errors - Total	

Additional Resources for Monitoring the Ethernet

Please make sure to read the following PDF documents uploaded to the course web.

1. Ethernet_errors.pdf *(5 pages)*
2. Troubleshooting_ethernet.pdf *(12 pages)*

Monitoring and analysis of the Network Traffic

Network Traffic

What & how should we measure..?

- Measure amount and type
  - ❑ Need hardware tools

What are possible types to monitor..?

- Number of Nodes/Users
- Protocols
- Broadcast/Multicast/Unicast
- Conversations
- Errors

Number of Nodes/Users

- Workstations
- Servers
- Peripherals
- Routers and switches
- Who is on the network
- Physical access

Protocols

- Device dependent
- Segment dependent

How much of your traffic is overhead protocols

ARP – Address Resolution Protocol

To find the physical address for a given logical address.

DNS – Domain Name Service

To find the IP address for a given domain name.

ICMP – Internet Control Message Protocol

One of the core protocols of the Internet Protocol Suite used primarily for the purpose of sending error messages.

How much of your traffic is overhead protocols

LDAP – Lightweight Directory Access Protocol

For the purpose of accessing and maintaining distributed directory information services.

RIP, EIGRP, OSPF etc.

For the purpose of managing network devices.

Connections

- Who is talking to who?
  - ❑ How much?
    - ➢ Routers
    - ➢ Servers

- Applications
  - ❑ What applications are on the network
  - ❑ What protocols are they using
  - ❑ Which users access them

Where do errors occur?

- 65% to 75% of network errors occur in the first three layers

- Causes
  - ❑ Duplicate addresses
  - ❑ Host/Station/Network unreachable
  - ❑ Time-To-Live (TTL) exceeded

Monitoring and analysis of Platforms and Operating Systems

Determining Server Workload Characterization

What is workload characterization..?

- Within the confines of a network, workload is the amount of work assigned to, or done by, a client, workgroup, server, or internetwork in a given time period.

- Therefore, workload characterization is the science that observes, identifies and explains the phenomena of work in a manner that simplifies your understanding of how the client, workgroup, server, or internetwork is being used.

Determining Server Workload Characterization

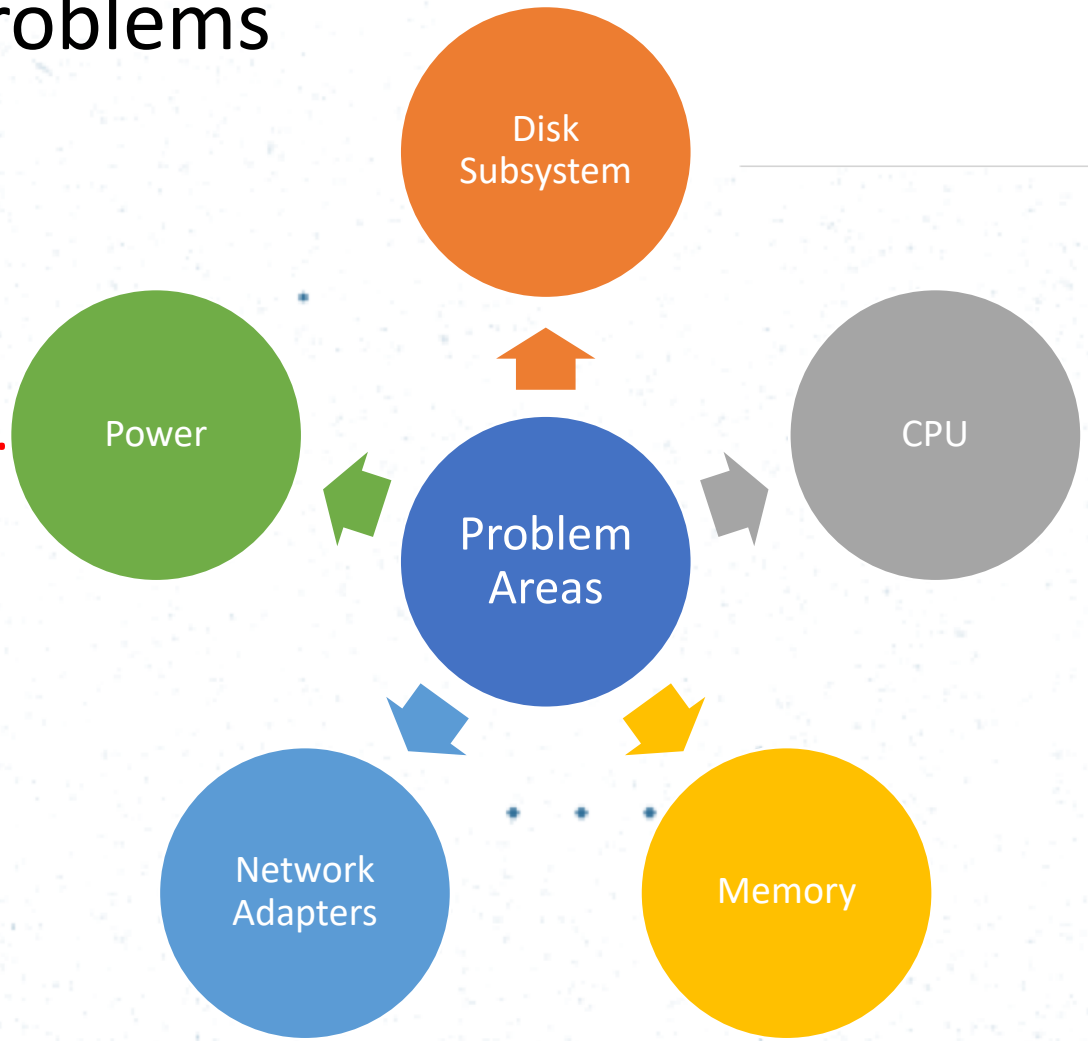
Things that should be considered..

- Server type
- Workload characterization
- Isolate components that restrict data flow
- Set expectations

What are common server problems

Problems can occur in..

Not covered.



What are common server problems

Disk Subsystem

- The disk subsystem is more than the disk itself.
- It will include,

- Problems can occur with any of the above components..!!

Note

In NT based windows server environments, the disk subsystem is divided into two part for ease of monitoring and troubleshooting.

- Physical disk - used for the analysis of the overall disk, despite the partitions that may be on the disk.
- Logical disk - analyzes information for a single partition.

What are common server problems

CPU

- Most server machines today, support 1-4, 1-8 or even 1-16 processors.
- And each processor can have up to 18 CPU cores.
- That is A LOT to monitor and troubleshoot..!!

Leads to common problems..

- Overheating due to not been correctly thermally bonded with heat sink during installation & replacement.
- Mismatches between CPU and memory speeds.
- Different CPUs populated with different number and size of memory modules.
- Etc.. Etc..

What are common server problems

Memory

- In server machines each processor can be populated with one or more memory modules.
- Some modern server stations even support up to 96 memory modules.

Leads to common problems..

- The number and size of modules not same for all CPUs in a server.
- Memory module not seated properly in the slot.
- Using modules having different speeds.
- Memory module not supported by the particular server model.
- Etc.. Etc..

What are common server problems

Network Adapters

- Some modern server stations can support a large number of NIC ports, even up to 16 ports.
- Larger the number of ports become, so does the complexity of troubleshooting..!!

Leads to common problems..

- Not loading the appropriate firmware version for the adapters.
- If/when using dual adapters, not following the restrictions on the supported combinations.
- Etc.. Etc..

File and Print Servers

- File and printer servers manage the storage of data and the various printers on the network.

  E.g. Windows Server 2008, Mac OS X Server, Red Hat Linux Server, Ubuntu Server Edition.

- **Key Concern**: Disk I/O or the number of user's attempting access to the server is the most critical concern.

- Focus on the number of users accessing server concurrently (also how they are accessing the server) and amount of resources demanded.

Web Servers

- Web servers allow Internet users to attach to your server to view and maintain web pages.

- Ordering of problem areas to focus,

  Memory > Network >

- Must fulfill requests from cache to achieve maximum performance.

Application Server

- Application server is a server that handles all application operations between users and an organization's backend business applications or databases. Aka *appserver*.
- Features include, built-in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access.
- Ordering of problem areas to focus,

  Memory >
- Application server usually has smaller, more frequent requests to it than File and Print Server environment.

Logon Server/System Services

- As the name implies, logon server is used for the purpose of authenticating users to the domain.
- Logon servers can provide convenient authentication features like Single Sign On (SSO), which enables the users to access multiple applications/services using the same username and password.
- Ordering of problem areas to focus,

  Processor > Disk
- Things to keep an eye on,
  - ❑ Activity generated between Servers.
  - ❑ Users - Peak activity more of a concern.

Why..?

Factors affecting performance

- Performance degradation is proportional to the problems.

- Hence, areas that problems can occur are the same areas that will affect performance.
  - ❑ Disk Subsystem
  - ❑ Memory
  - ❑ CPU
  - ❑ Network

Common Hard Disk Measurements

- Current Disk Queue Length
- % Disk Time
- Avg. Disk Queue Length
- Disk Reads/sec
- Disk Reads Bytes/sec
- Avg. Disk Bytes/Transfer
- Avg. Disk sec/Transfer

Paging and Swapping

Paging

- Move individual pages of process to the disk to reclaim memory.
- The paging algorithm keeps track of when each page was last used and tries to keep pages that were used recently in memory.

Swapping

- Move an entire process to disk to reclaim memory.
- Next time the system runs the process, it has to copy it from the disk swap space back into memory.

Revisit OS lecture slides..

Common Memory Measurements

- Page Faults/sec
- Pages Input/sec
- Pages Output/sec
- Pages/sec
- Page Reads/sec
- Page Writes/sec
- Available Memory
- Nonpageable memory pool bytes
- Pageable memory pool bytes
- Committed Bytes
- Pool Paged Bytes
- Pool NonPaged Bytes
- Working Set
- Paging File, %pagefile in use

Common Processor (CPU) Measurements

- % Processor Time
- Interrupts/sec
- % Interrupt Time
- % User Time
- % Privilege Time
- % DPC Time
- % Processor Time
- Processor Queue Length
- System Calls/sec
- % Total Processor Time
- % Total User Time
- % Total Privilege Time
- % Total Interrupt Time

Common Network Card Measurements

- Bytes Sent/sec
- Bytes Received/sec
- Bytes Total/sec
- % DPC Time
- DPCs queued/sec
- % Broadcasts
- % Multicasts
- Segments Sent/sec
- Segments Received/sec
- Segments/sec
- Segments Retransmitted/sec
- Connection Failures
- Connections Reset
- Connections Established
- Server Sessions
- Output Queue Length

Further reading..

If you are interested in knowing some further information about performance counters you can refer the following PDF uploaded to moodle,

Performance_Counters.pdf

Don’t overdo it…!!!

Excessive network monitoring (active) can and will slow your network…!!!

~ THE END ~