Network and Service Monitoring

Topics

- Monitoring and prediction
- Underlying solutions
  - SNMP
  - WBEM
  - WMI
  - Netflow (IPFIX)
- Monitoring Information Storage
  - SQL, RRD

Monitoring

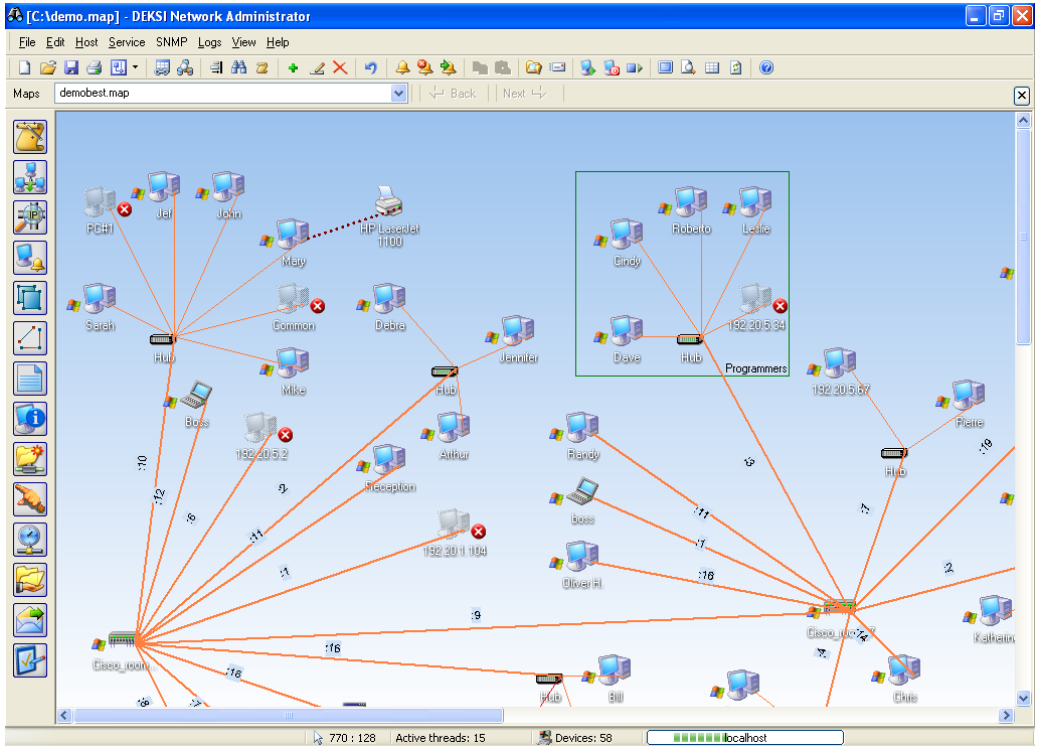
- **Monitoring** describes the use of a system that constantly monitors a computer, a network or device for variations on the normal functioning of a systems and that notifies the administrator/manager in case of outages/ disruptions via email, SMS or other alarms. It is a subset of the functions involved in network management.

Motivation

- Needs of service providers:
  - Understand the behavior of their networks
  - Provide fast, high-quality, reliable service to satisfy customers and thus reduce churn rate
  - Plan for network deployment and expansion
  - SLA monitoring, Network security
  - Usage-based billing for network users (like telephone calls)
  - Marketing using CRM data
- Needs of Customers:
  - Want to get their money's worth
  - Fast, reliable, high-quality, secure, virus-free Internet access

Monitoring

- Passive Analysis
- Active Probing



Passive Analysis

- Carried out by observing network traffic
  - Collect packets from a link or network flow from a router
  - Perform analysis on captured packets for various purposes
  - Network device performance degrades by mirroring or flow export
- Used to perform various traffic usage/ characterization analysis/intrusion detection

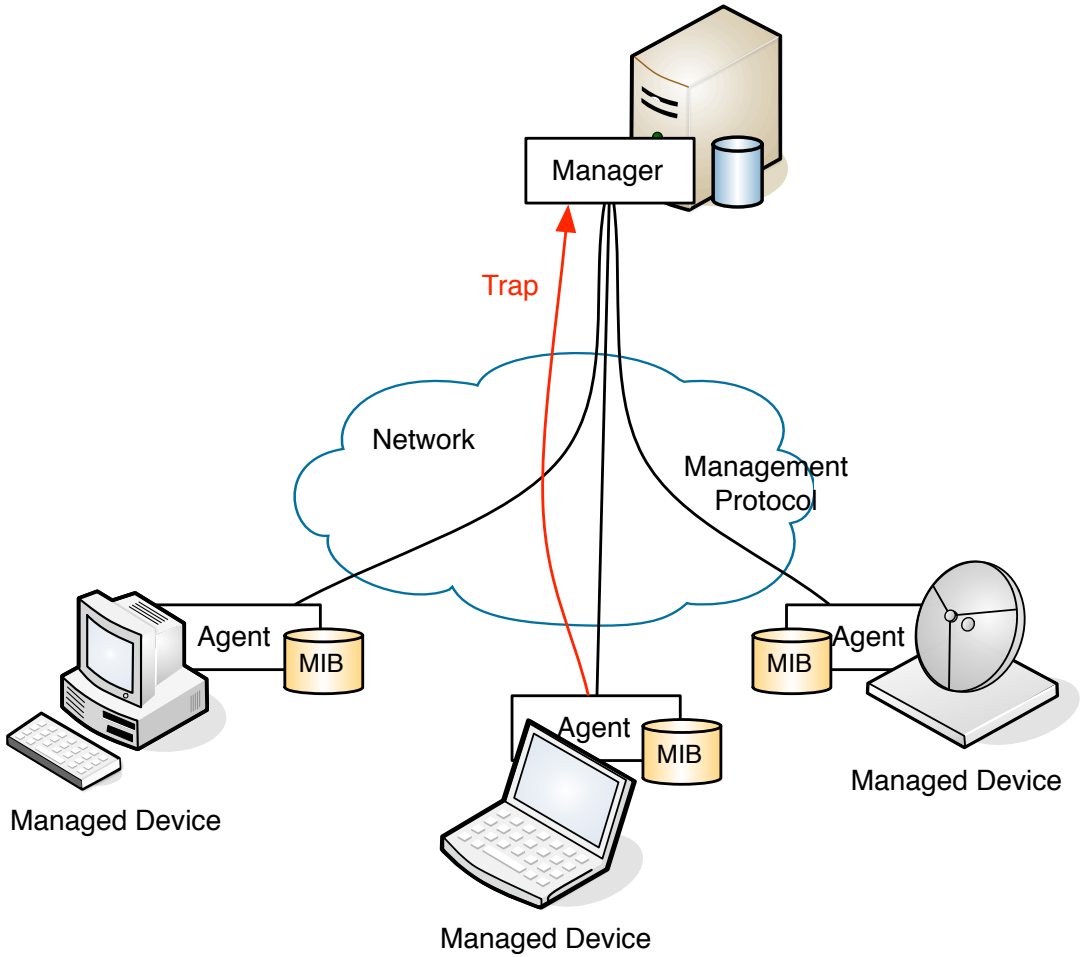
Active Monitoring

- Performed by sending test traffic into network
  - Generate test packets periodically or on-demand
  - Measure performance of test packets or responses
  - Take the statistics
- Impose extra traffic on network and distort its behavior in the process
- Test packet can be blocked by firewall or processed at low priority by routers
- Mainly used to monitor network performance

Concepts

- Managed Device (MD): A device which can be managed by some other system
- Agent: A software device running on a MD.
- Management Information Base (MIB): The specification of the management data on a MD
  - Ex: TCP/IP MIB, BLDG-HVAC-MIB
- Management Station: A software managing agents
- * Management System: A complete solution to manage a domain
  - Ex: Network Management System (NMS)
- Trap: An asynchronous message sent by agents due to some event
  - Ex: cable disconnected, temperature threshold exceeded

Management System



Metric Scope

- Infrastructure
  - Network: equipment, network devices and links
  - HVAC: equipment, consumption
  - Servers: equipment and base OS
- Application
  - System usage: CPU, Memory, IO
- Service
  - Service usage: requests, DB accesses

Metric types

- Higher is Better
  - Threshold represents a lower bound for data
  - Ex: Availability, Throughput
- Lower is Better
  - Threshold represents an upper bound for data
  - Ex: Temperature, Humidity, Loss, Latency
- Nominal is Better
  - Threshold for both upper and lower bounds
  - Ex: Utilization. High = saturation, low = underusage

Common Metrics

- Throughput: requests / unit of time
  - Bytes/s, IOPS, Hits/s, Queries/s
- Utilization: used time / free time
- Reliability: Probability of error
- Availability: available time / downtime
- Mean uptime: Mean Time Before Failure

SNMP

- SNMP is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices.
- Application-layer protocol for managing TCP/IP based networks.
- UDP based protocol

SNMP Advantages

- Standardized
- universally supported
- extendible
- portable
- allows distributed management access
- lightweight protocol

The Three Parts of SNMP

- SNMP Protocol
  - Defines format of messages exchanged by management systems and agents.
  - Specifies the Get, GetNext, Set, and Trap operations
- Structure of Management Information (SMI)
  - Rules specifying the format used to define objects managed on the network that the SNMP protocol accesses
- Management Information Base (MIB)
  - A map of the hierarchical order of all managed objects and how they are accessed

SNMP Components

- **Management Information Base**: Referred to as the MIB, this is the management data which can be exchanged between the different SNMP components. The MIB consists of individual objects, which can be referred to by their numerical Object Identifier (OID) or their textual Object Descriptors. An example of this is the system MIB, supported by the SNMP agent. The following is one of the objects within the system MIB:

  sysDescr / 1.3.6.1.2.1.1.1

- sysDescr is the Object Descriptor, whereas 1.3.6.1.2.1.1.1 is sysDescr's OID.

Basic SNMP Components

- **Agent***:* This is the primary SNMP component. The agent is responsible for a basic MIB (containing system and agent specific information), accepting queries from managers, forwarding queries to subagents, and sending out traps.
- **Manager***:* This is the SNMP component from which requests are generated for agent and subagent MIB objects. The manager can query MIB objects, and can also set the value of some objects.
- **Subagent***:* This component is typically part of another application, and supports a MIB which contains objects specific to that application.

SNMP Communities

- Community names are used to define where an SNMP message is destined for.
- They mirror the same concept as an Active Directory Domain or Unix domain.
- Set up your agents to belong to certain communities.
- Set up your management applications to monitor and receive traps from certain community names.

SNMP Operations

- Get
  - Retrieves the value of a MIB variable stored on the agent machine (integer, string, or address of another MIB variable)
- GetNext
  - Retrieves the next value of the next lexical MIB variable
- Set
  - Changes the value of a MIB variable
- Trap
  - An unsolicited notification sent by an agent to a management application (typically a notification of something unexpected, like an error)

The SNMPv1 Security Model

- SNMP supports three security models:
  - SNMPv1, SNMPv2c, and SNMPv3
- SNMPv1 is a "community based" security environment
- In a community based model, the SNMP agent authenticates requests based on the following:
  - A community name, which acts like a password
  - The IP address (or subnet address) associated with the community name which must correspond with the IP address of the manager's host
  - Note that the requests—including the community name—are sent unencrypted.
    - Anyone with a sniffer or packet trace can capture the request and determine the community name

Languages of SNMP

- Structure of Management Information (SMI)
  - specifies the format used for defining managed objects that are accessed via the SNMP protocol
- Abstract Syntax Notation One (ASN.1)
  - used to define the format of SNMP messages and managed objects (MIB modules) using an unambiguous data description format
- Basic Encoding Rules (BER)
  - used to encode the SNMP messages into a format suitable for transmission across a network

SMI Structure of Management Information

- SMIv2 is described in RFCs 1442, 1443, 1444
- These RFCs describe:
  - How MIB modules are defined with CCITT X.208 ASN.1 data description language
  - The subset of the ASN.1 language that is used in MIBs
  - The addition of the APPLICATION data type to ASN.1, specifically for use with SNMP MIBs
  - All ASN.1 constructs are serialized using the CCITT X.209 BER for transmission across the wire
  - definition of the high-level structure of the Internet branch (iso(1).org(3).dod(6).internet(1)) of the MIB naming tree
  - the definition and description of an SNMP managed object

ASN.1 & BER

- ASN.1 (Abstract Syntax Notation One) is nothing more than a language definition. It is similar to C/C++ and other programming languages.
- BER (Basic Encoding Rules)
  - The relationship between ASN.1 and BER parallels that of source code and machine code.
  - CCITT X.209 specifies the Basic Encoding Rules
  - All SNMP messages are converted / serialized from ASN.1 notation into smaller, binary data (BER)

SNMP Data Types

- INTEGER -- signed 32-bit integer
- OCTET STRING
- OBJECT IDENTIFIER (OID)
- NULL -- not actually data type, but data value
- IpAddress -- OCTET STRING of size 4, in network byte order (B.E.)
- Counter -- unsigned 32-bit integer (rolls over)
- Gauge -- unsigned 32-bit integer (will top out and stay there)
- TimeTicks -- unsigned 32-bit integer (rolls over after 497 days)
- Opaque -- used to create new data types not in SNMPv1
- DateAndTime, DisplayString, MacAddress, PhysAddress, TimeInterval, TimeStamp, TruthValue, VariablePointer -- textual conventions used as types

Commercial SNMP Applications

- **http://www.hp.com/go/openview/ HP OpenView**
- **http://www.tivoli.com/ IBM NetView**
- **http://www.novell.com/products/managewise/ Novell ManageWise**
- **http://www.sun.com/solstice/ Sun MicroSystems Solstice**
- **http://www.microsoft.com/smsmgmt/ Microsoft SMS Server**
- **http://www.castlerock.com/ Castle Rock Computing**

Other Monitoring Protocols

- WBEM (Web Based Enterprise Management)
  - Developed by DMTF (Distributed Management Task Force)
  - Built on top of the Common Information Model (CIM)
- WMI (Windows Management Interface)
  - MS version of WBEM
- Windows Remote Registry
  - In addition to WMI, Microsoft provides a Remote Registry interface to getting system information from the performance registry remotely
  - The protocol for the remote registry is RPC (Remote Procedures Call) and introduces challenges in terms of network connectivity and platform independent client tools
- Agentless monitoring by sending system commands over the network

WMI

Netflow (IPFIX)

CIM

- Object-oriented information model
  - Provides a conceptual framework for describing management data
    - For computing and business entities
    - In Internet, enterprise and service provider environments
  - Formalism
    - UML – Universal Modeling Language
    - MOF – Managed Object Format
- CIMOM – CIM object manager
  - Implements CIM
  - WMI includes a CIMOM component

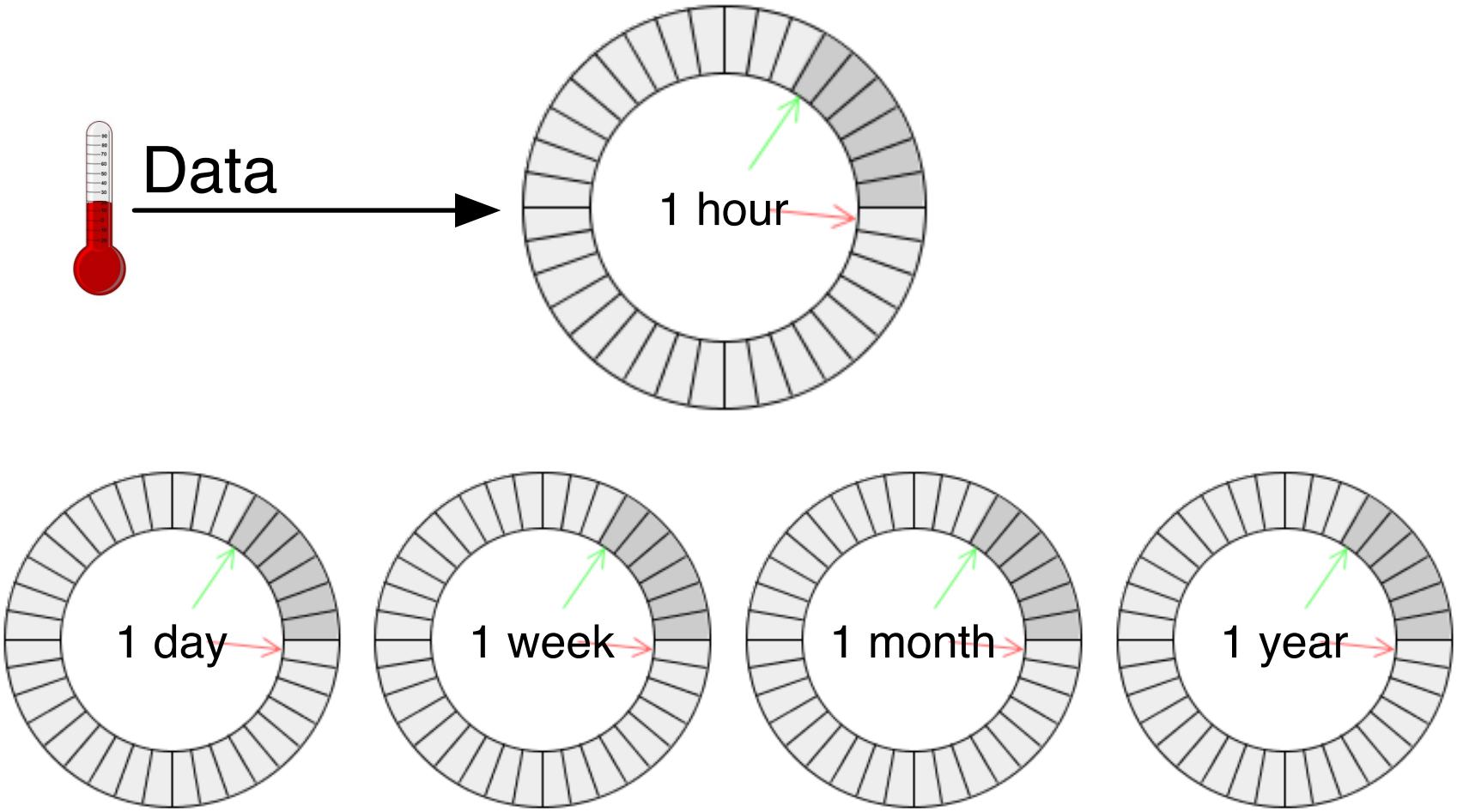
Round Robin Databases (RRD)

- Monitoring produces large amount of information
  - 1 record produced each monitoring period
    - 1 minute interval: 1440 records per day
  - Single server can have tens of metrics
    - Memory, latency, load, storage, power, fans, traffic, etc…
  - Services may require even more monitoring metrics
    - Remember: TIER IV requires 99.995% availability (24min/y).

Round Robin Databases (RRD)

- Based on databases of circular tables for periodic data
  - Old data is overwritten by new data
  - Database size is limited
  - Automatically deals with data aging
- Limited to numerical data
  - Supports floating point
  - Missing values are interpolated
  - Actual data stored differs from inserted
- Frequently organized in hierarchical views
  - Day, week, month, year, views etc…

Round Robin Databases (RRD)



RRD Concepts

- Round Robin Archive (RRA): A timeseries inside a RRD database
- Steps: Time interval of the RRA. Ex: 300s, 3600s
- Primary Data Point (PDP): A value
- Consolidation Function (CF): A function applied to PDP. Ex: Average, Maximum, Minimum
  - Possible to define custom CF (CDEF): CDEF:dataBytes=dataBits,8,*

RRD Concepts

- Consolidated Data Point (CDP): The result of applying a CF to a PDP
- Data Source (DS): A source of data. Ex: temp
- Data Source Type (DST): How to store data
- X Files Factor (XFF): Percentage of missing records

RRD DST

Counter: Rate of change (pos values)

Derive: Rate of change (pos and neg values)

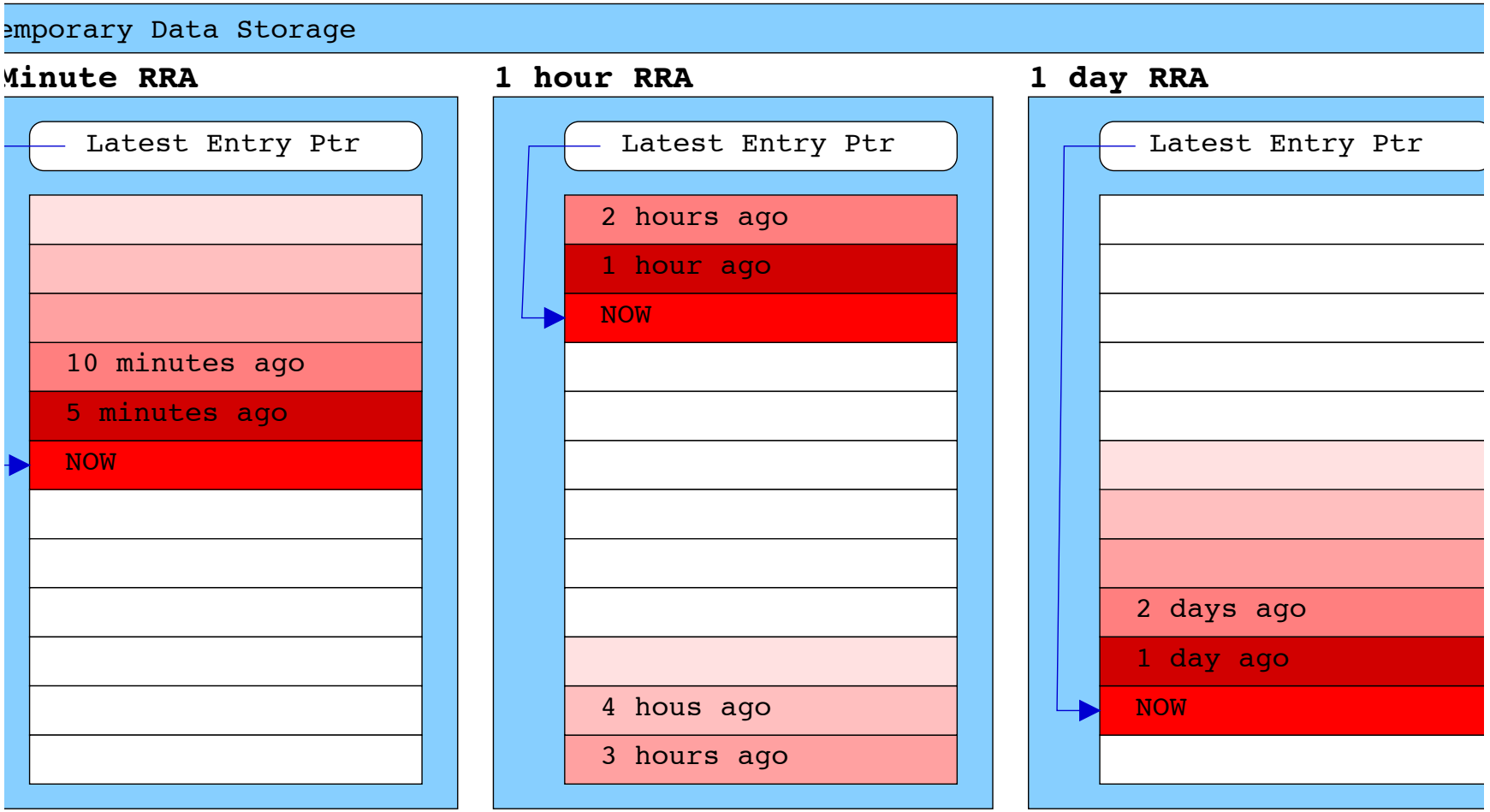
Absolute: Rate of change for base step

Gauge: Actual Value

```
Values          = 300, 600, 900, 1200

Step            = 300 seconds
COUNTER DS      = 1, 1, 1, 1
DERIVE DS       = 1, 1, 1, 1
ABSOLUTE DS     = 1, 2, 3, 4
GAUGE DS        = 300, 600, 900, 1200
```

Round Robin Databases (RRD)

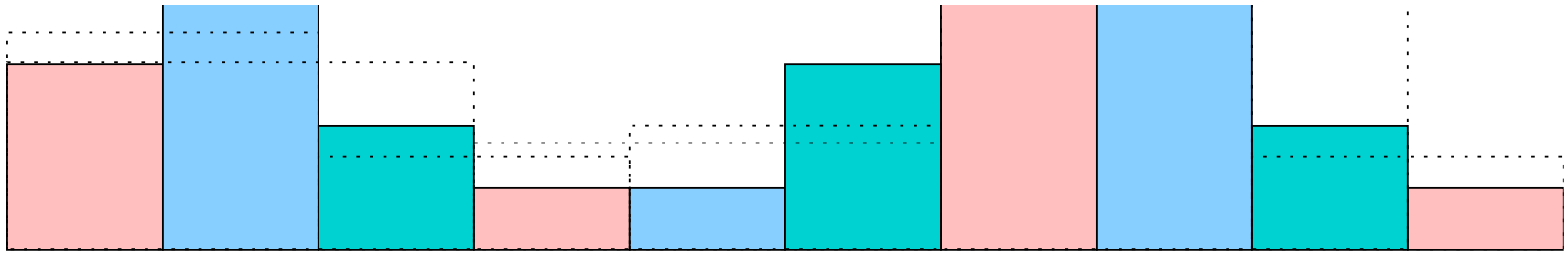


RRD: RRD Creation

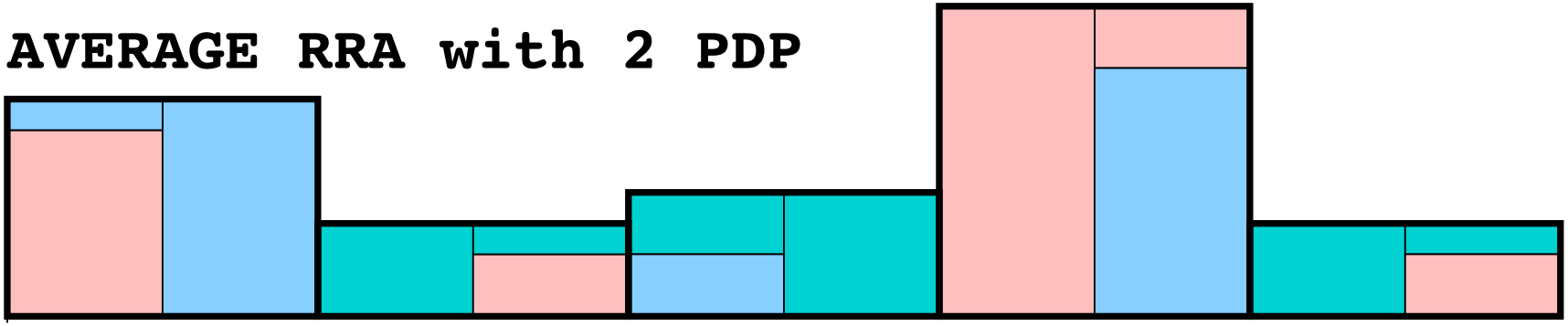
- RRD creation must define
  - Name, Start Time and Step:
  - Data Source and Data Source Type
  - RRA defining extra CDP
    - Format: CDF:X Files Factor:num steps for cdf:num records
    - XFiles Factor: min percentage of steps required

```
rrdtool create room220-temp.rrd\
         --start 1315330982\
         --step 300 \
         DS:temp:GAUGE:600:0:70\
         RRA:AVERAGE:0.5:12:24 \
         RRA:AVERAGE:0.5:288:31
```

RRD: RRA

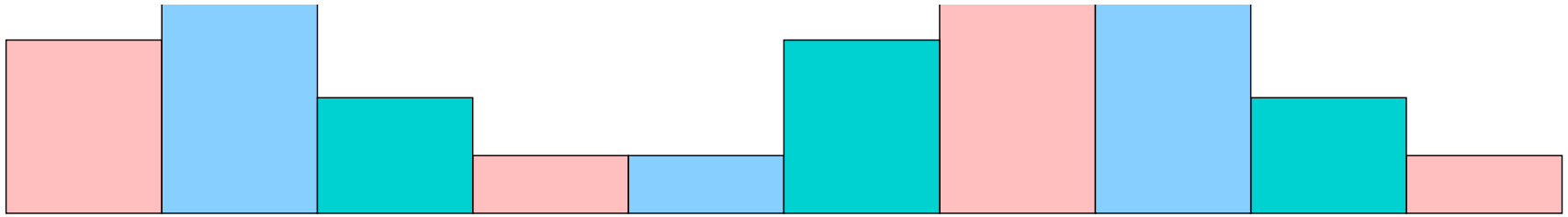


AVERAGE RRA with 2 PDP

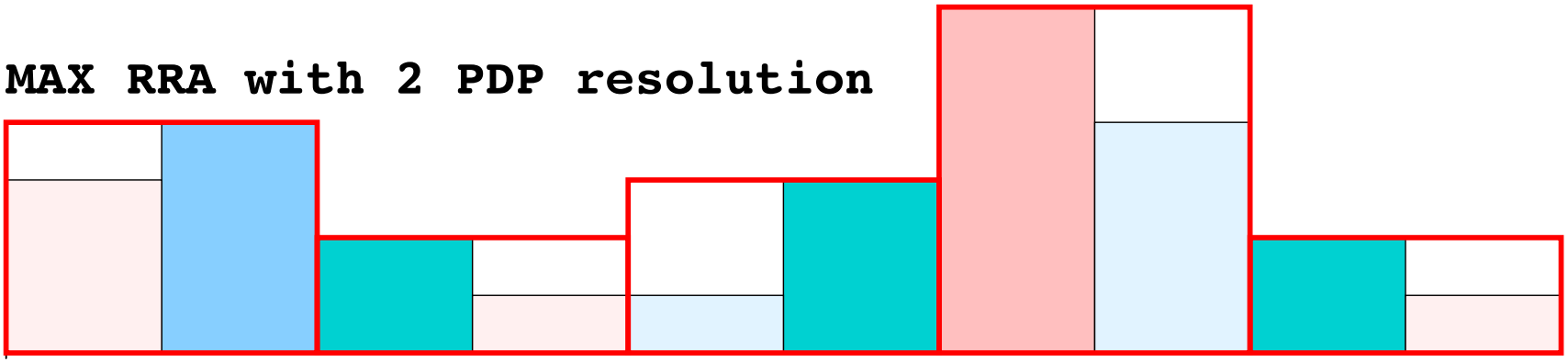


AVERAGE RRA with 3 PDP

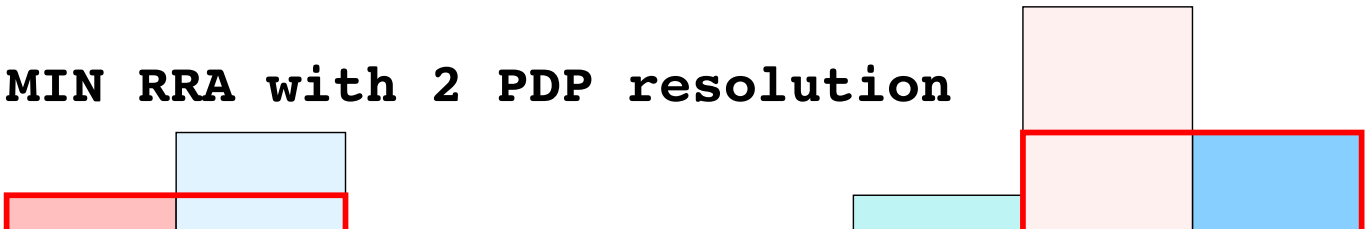
RRD: RRA



MAX RRA with 2 PDP resolution



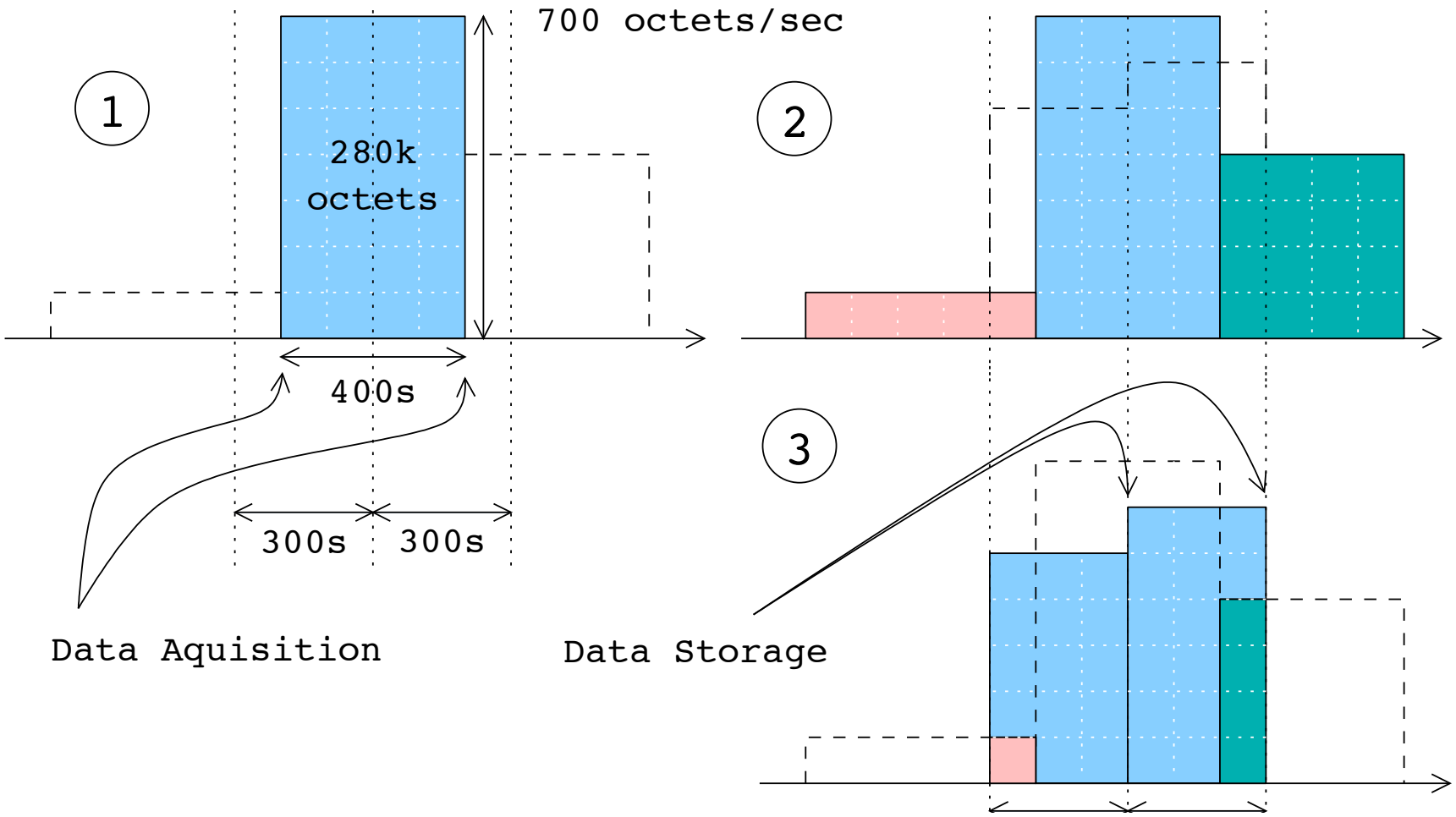
MIN RRA with 2 PDP resolution



RRD: Data Re-Binning

- RRD expects monotonic timeseries
  - Ex: 1 value each 300s
- What if input is not monotonic?
  - Ex: 1 value each 300s, then 1 value 400s later
- Missing data is interpolated
  - After XFF, UNKNOWN string is stored

RRD: Data Re-Binning



Storage Management Principles

- Monitoring
- Reporting
- Provisioning

Storage Monitoring

- Monitoring – Collect information about key parameters
  - Performance – may vary with usage pattern
  - Capacity – usually keeps increasing
  - Accessibility – availability due to events
  - Others: temperature, IOPS, etc..
- Data collected and stored in databases

Storage Reporting

- Reporting – generate reports periodically
  - Based on monitoring data
  - Provide information about the status of a specific moment in time
- Reports may trigger correction actions
  - Performance at 16h is unacceptable
- Reports may provide indication about effectiveness of changes
  - Ex: Performance increased or decreased

Storage Provisioning

- Provisioning – Plan ahead the needs
  - Take in consideration evolution across different reports
  - Storage provisioning focused in resources and capacity
- Capacity Planning – Plan ahead the capacity needs
  - A steady increase is the norm
  - Must be done with months (years) in advance
- Resource Planning – Plan ahead the resources needed
  - Technology, personal, security