



# Big Brother in the Access Network: Monitor Service Enablers for IPTV Services

**Bart De Vleeschauwer & Filip De Turck**  
Ghent University – IBBT-IMEC  
Department of Information Technology  
[Bart.DeVleeschauwer@intec.ugent.be](mailto:Bart.DeVleeschauwer@intec.ugent.be)



**MUSE Autumn School 2006**  
**(October 19-20, Bilbao)**

- > The “Internet” has changed...
- > Web traffic -> Multimedia Services
  - VOIP
  - Video On Demand
  - IPTV
  - High Speed Internet
  - Peer-to-peer networks
  - Online Gaming
- > QoE is becoming more and more important
- > Monitoring is essential for detecting network and QoE problems

# Home Network and Services Evolution



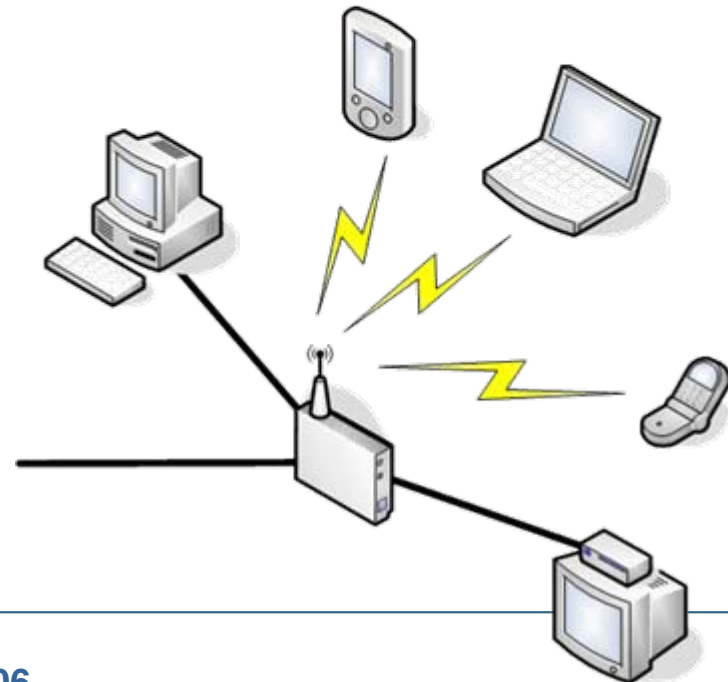
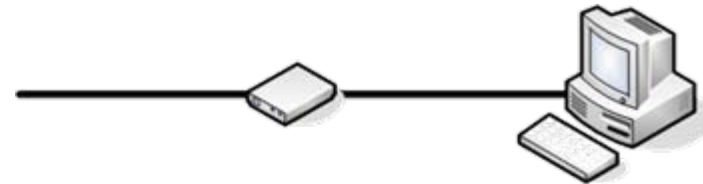
- > A decade ago
  - Desktop PC
  - 56.6 kbit/sec access line
  - Services
    - WebSurfing
    - File transfer
    - Email

} Best Effort

- > Today
  - Large Home Network
    - Set Top Boxes
    - Portable devices, PDAs,...
    - Desktop PCs
    - Wireless network
  - Multi megabit/sec access line
  - Myriad of services
    - IPTV
    - VOIP
    - HSI
    - WebSurfing
    - Email
    - File transfer
    - ...

} Require QoS

} Best Effort



- > The new network is required
  - Service rich
  - Dependable
  - Highly flexible
- > Former architecture
  - Intended for best-effort HSI
  - High oversubscription

# Why triple play?



## > Why triple play ?

- Telco's core wired voice service is eroding
- Big market
- Triple play is the first step towards converged networks
- Technology is now able to provide these services
  - Encoding has evolved
  - Access networks have evolved

## > IPTV operator incentives

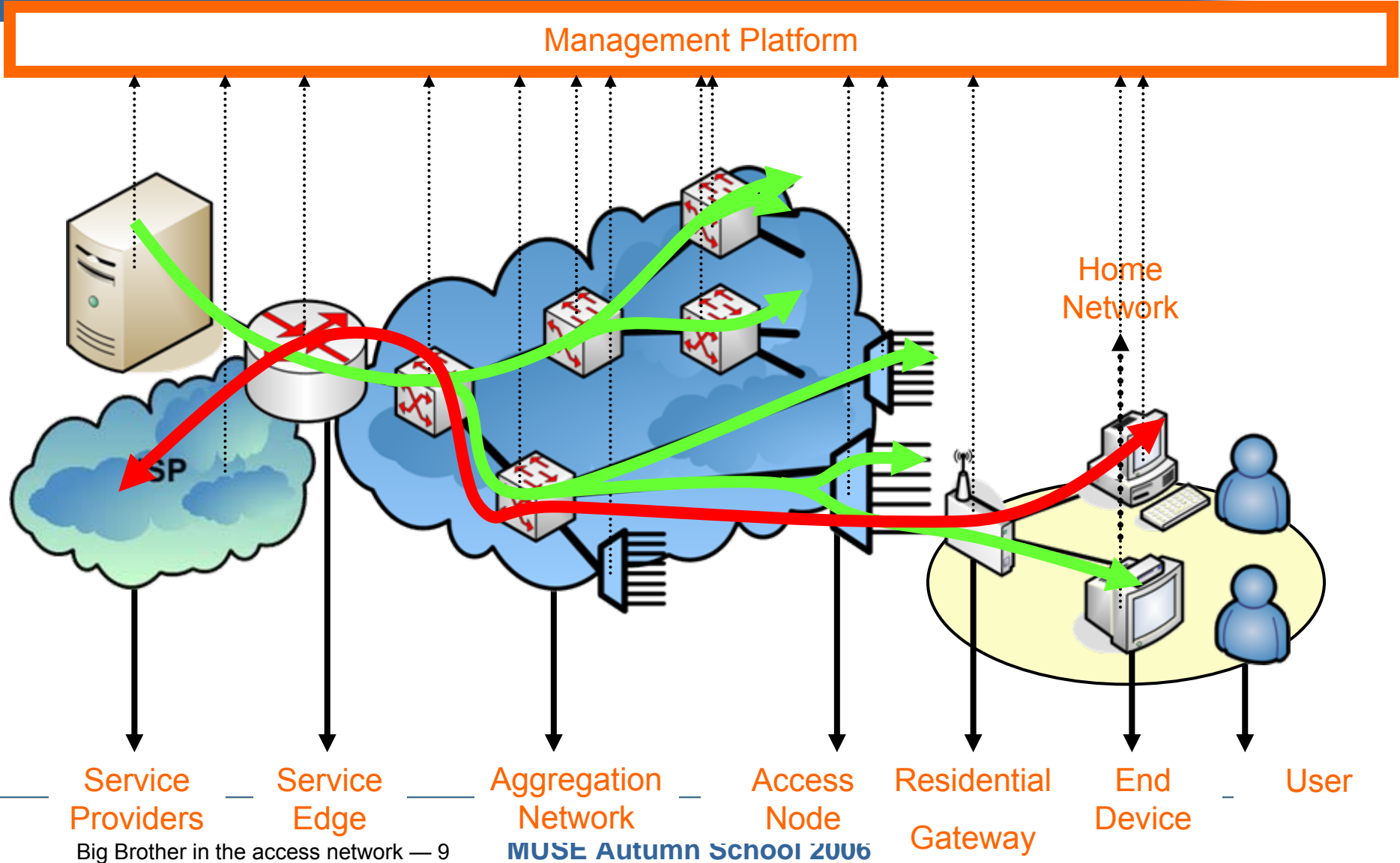
- Huge customer potential (Alcatel estimate: 72,000,000 IPTV subscribers by 2010)
- Big increase in ARPU (x2/x3)

- > New services are very sensitive to network problems
  - Delay
  - Jitter
  - Packet loss (IPTV: loss must be lower than  $10^{-6}$ )
- > Video sensitivity to packet loss (Demo)
- > Conclusion: Even small amounts of packet loss have impact on QoE!
- > The success of the new services is tightly related to the QoE of these services!
- > Monitoring factors that can impact this QoE and detecting problematic behavior is of prime importance.

- > To react to QoE degradation, monitoring plays a central role to detect problems
- > Possible reactions include:
  - Reconfiguring network devices
  - Triggering application specific actions
    - Forward error correction
    - Interleaving
    - Retransmission

- > **Access network overview**
- > Network monitoring techniques
- > Monitoring data analysis
- > Advanced multimedia services
  - IPTV
- > The RTP/RTCP protocol
- > DSLForum
- > Raqmon
- > Conclusion

# Access Network Overview



- > Access network overview
- > **Network monitoring techniques**
- > Monitoring data analysis
- > Advanced multimedia services
  - IPTV
- > The RTP/RTCP protocol
- > DSLForum
- > Raqmon
- > Conclusion

# ICMP Based Active Measurements

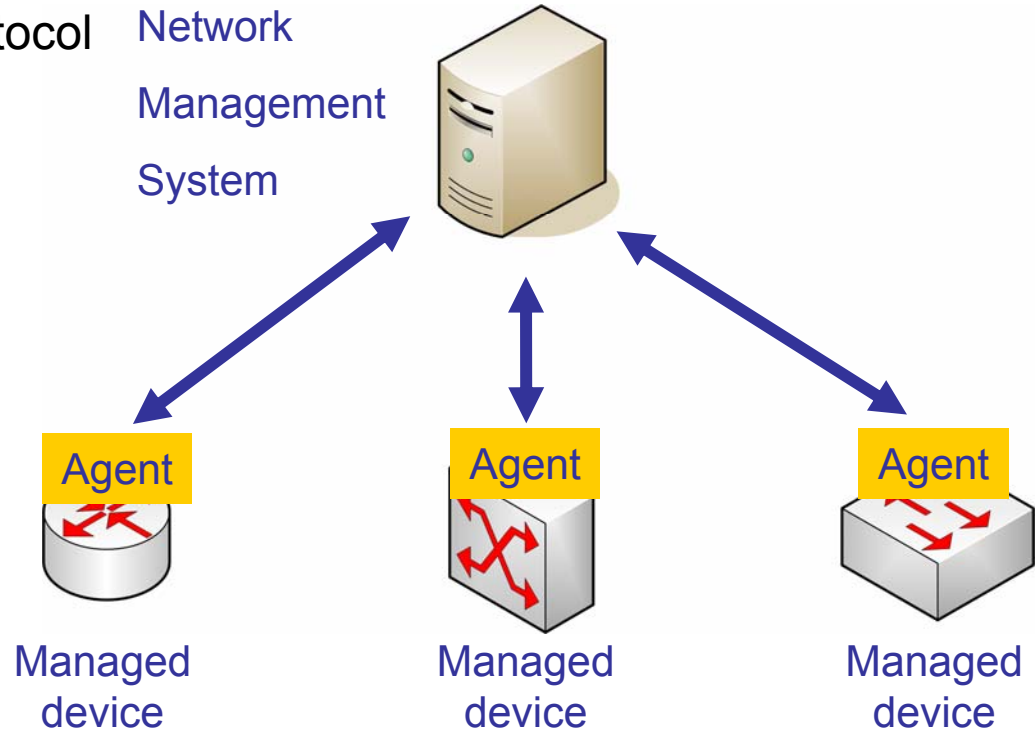


- > RFC 792: Internet Control Message Protocol (ICMP)
- > Send packets between hosts and observe behavior of these packets
- > Gives end-to-end information
- > Ping/Traceroute
- > Supported on any Internet device
- > Can be used for:
  - Connectivity
  - RTT
  - Packet loss
  - Jitter
  - Number of hops
  - (One way delay)
- > Possible issue: NA

```
C:\>ping -n 10 ibcn.intec.ugent.be
Pinging ibcnweb.intec.ugent.be [157.193.173.245] with 32 bytes of data:
Reply from 157.193.173.245: bytes=32 time=1ms TTL=62
Reply from 157.193.173.245: bytes=32 time=2ms TTL=62
Reply from 157.193.173.245: bytes=32 time<1ms TTL=62
Reply from 157.193.173.245: bytes=32 time<1ms TTL=62
Reply from 157.193.173.245: bytes=32 time<1ms TTL=62
Reply from 157.193.173.245: bytes=32 time<1ms TTL=62
Reply from 157.193.173.245: bytes=32 time<1ms TTL=62
Reply from 157.193.173.245: bytes=32 time=1ms TTL=62
Reply from 157.193.173.245: bytes=32 time=1ms TTL=62
Reply from 157.193.173.245: bytes=32 time=1ms TTL=62
Ping statistics for 157.193.173.245:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Estimate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
```

# SNMP

- > **Simple Network Management Protocol**
- > Application layer protocol
- > Two elements:
  - Network management system
  - Managed device
- > Allows to:
  - Manage performance
  - Solve problems
  - Plan for network growth
- > Basic commands:
  - Read
  - Write
  - Trap
  - Traversal operations
- > SNMPv1 (rfc1155) → SNMPv2 → SNMPv3



- Security
  - Authentication
  - Encryption
  - Access control

Request/Response

Bulk transfer

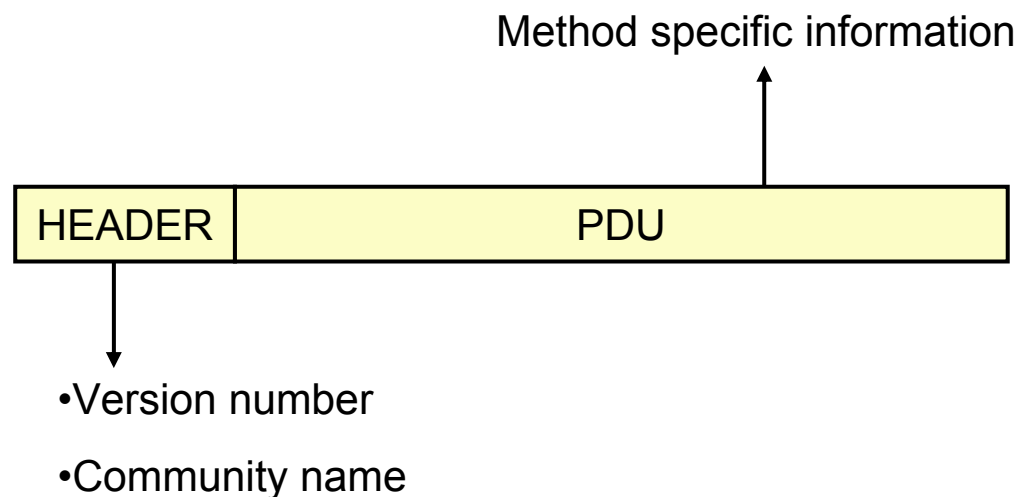
- > The SNMP framework consists of 4 components:
  - A data definition language
    - Structure of Management Information (SMI)
    - Data types
    - Object models
    - Writing rules
  - Definitions of management information
    - Management information base (MIB)
    - Object definitions
    - Event notification definitions
  - A protocol definition
    - Packets are sent over UDP and contain a header and a PDU
  - Security and administration

- > Object models: **Management Information Base (MIB)**
  - Hierarchically structured
- > Managed objects
  - Specific characteristic of a managed device
  - Two object types
    - Scalar (Single object instance)
    - Tabular (multiple related object instances, grouped in MIB table)
  - Identified using object identifier
- > Extendible
- > Many MIBs are available

# SNMP Messages



- > **GetRequest**
  - Generates Response upon receipt
- > **GetNextRequest**
  - For traversal of tables etc.
- > **Trap**
  - Generated on behalf of notification originator application
  - For notification of event
- > **Response**
  - Reaction to request...
- > **GetBulkRequest**
  - Large amount of data
- > **SetRequest**



- > rmonmib IETF working group
- > Family of RFCs that define a partition of MIB for use with network management
- > Provide interface between RMON agent and RMON management applications
- > Goals of RMON
  - Offline operation
  - Pro-active monitoring
  - Problem detection and reporting
  - Value added data
  - Multiple managers for one managed device
- > RFCs: 3577, 2819, 2021, ...

# RMON groups in rfc 2819



- > Ethernet statistics
- > History control (periodical statistical sampling)
- > Ethernet history
- > Alarm (thresholds)
- > Host
- > hostTopN
- > Matrix
- > Filter
- > Packet capture
- > Event

**Focus on Data Link Layer**

- > Protocol directory
- > Protocol distribution
- > Address mapping
- > Network layer host
- > Network layer matrix
- > **Application layer host**
- > **Application layer matrix**
- > User History

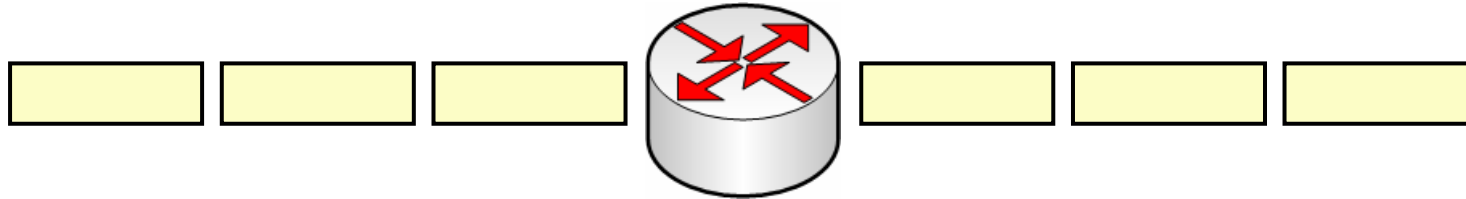
**Also contains information  
on communication between  
Applications and hosts**

- > Developed by Cisco
  - > Beyond SNMP
    - Characterize traffic applications and patterns
    - More granular understanding of bandwidth usage
    - Understanding who is communicating
  - > Monitor network flows
  - > IP flow fields (7):
    - IP source address
    - IP destination address
    - Source port
    - Destination port
    - Layer 3 protocol type
    - Class of service
    - Router or switch interface
- } Flow Identification

# Netflow functionality



Netflow enabled device



Source IP Address
Destination IP Address
Source Port
Target Port
Layer 3 protocol
TOS byte (DSCP)
Input Interface

Netflow cache

Flow Information	Packets	Bytes/packet

Additional information:

- Timestamp
- Next hop IP address
- Subnet mask
- TCP flags

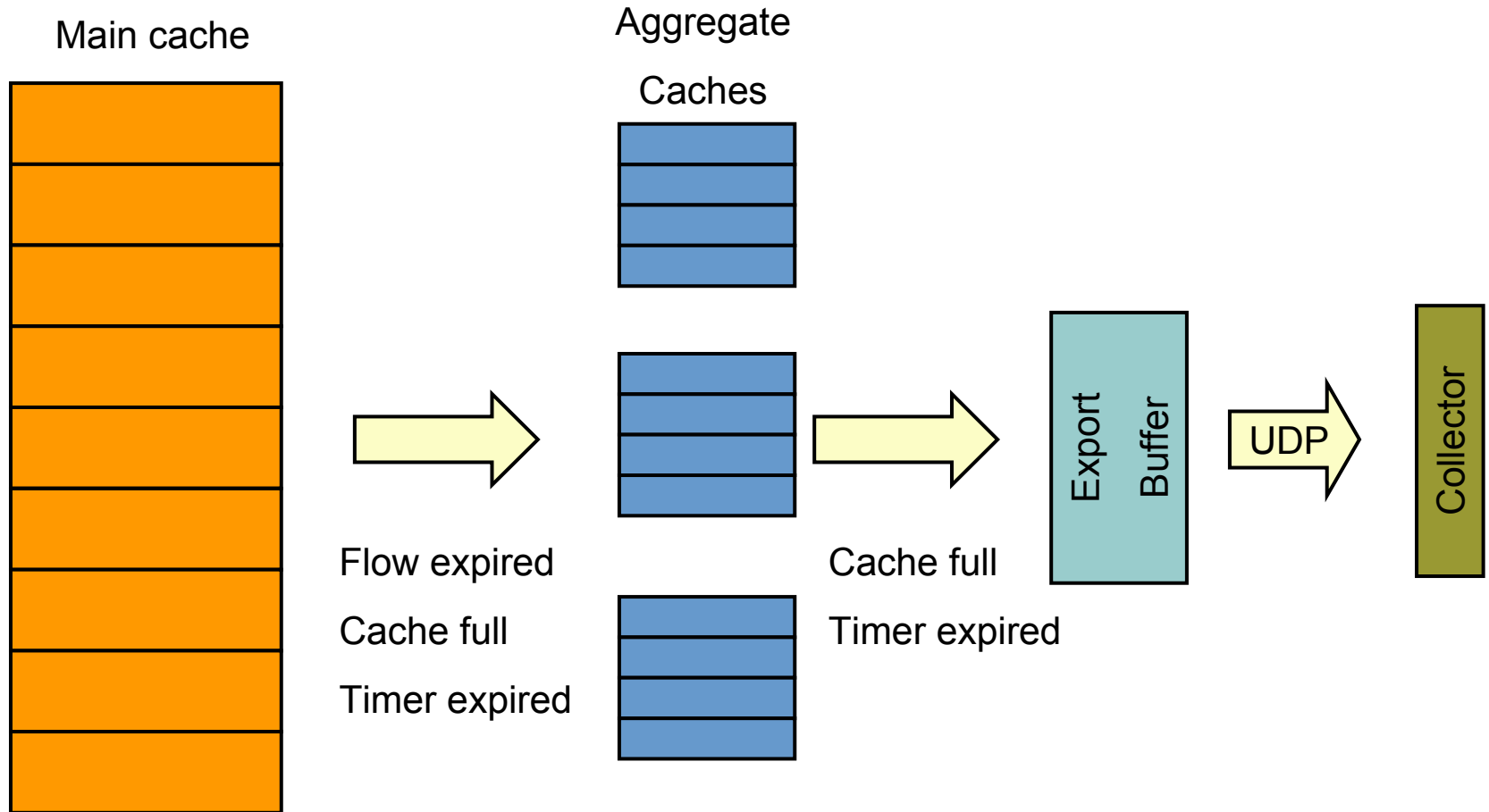
# Netflow data export and access



- > Flow information can be accessed in two ways
  - Command line interface (CLI)
  - Netflow collector
  
- > Flows are sent to collector
  - Bundle of 30-50 flows
  - Typically over UDP
  - Flow is inactive (15 seconds)
  - Timer is exceeded (30 minutes)

- > Sampling (only select fraction of all the packets)
  - Deterministic sampling (every Nth packet is selected)
  - Time based sampling (a packet is selected every N milliseconds)
  - Random sampling (one out of every N packets is selected)
- > Flow data aggregation: Summarize data on the Netflow enabled device
  - AS: AS-to-AS traffic flow data
  - Destination-prefix: Data flows with same destination prefix, destination prefix mask, destination BGP AS, output interface
  - Prefix: Same source prefix, source prefix mask, destination prefix, destination prefix mask, source BGP AS, destination BGP address, interfaces
  - Protocol Port: same IP protocol, source protocol number, destination port number (if applicable)
  - Source prefix:...
  - AS ToS:...
  - Destination Prefix ToS:...
  - Prefix ToS:...
  - Protocol Port ToS:...
  - Source Prefix ToS:...
  - Prefix Port:...

# Netflow data aggregation



- > IP Flow Information Export
- > The IETF ipfix working group
- > IP Flow
  - Set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to one flow share a set of properties. These properties are the result of applying a function to the values of:
    - One or more packet header fields (e.g. IP destination)
    - One or more characteristics of the packet itself (e.g. MPLS label)
    - One or more of fields derived from the packet treatment (e.g. next hop IP address)
  - A flow does not need to match an application level end-to-end stream
- > Applicability
  - Usage-based accounting
  - Traffic profiling
  - Traffic engineering
  - Attack/intrusion detection
  - QoS monitoring

# An IPFIX Device



Timestamping

Classification into flows

Sampling

Filtering

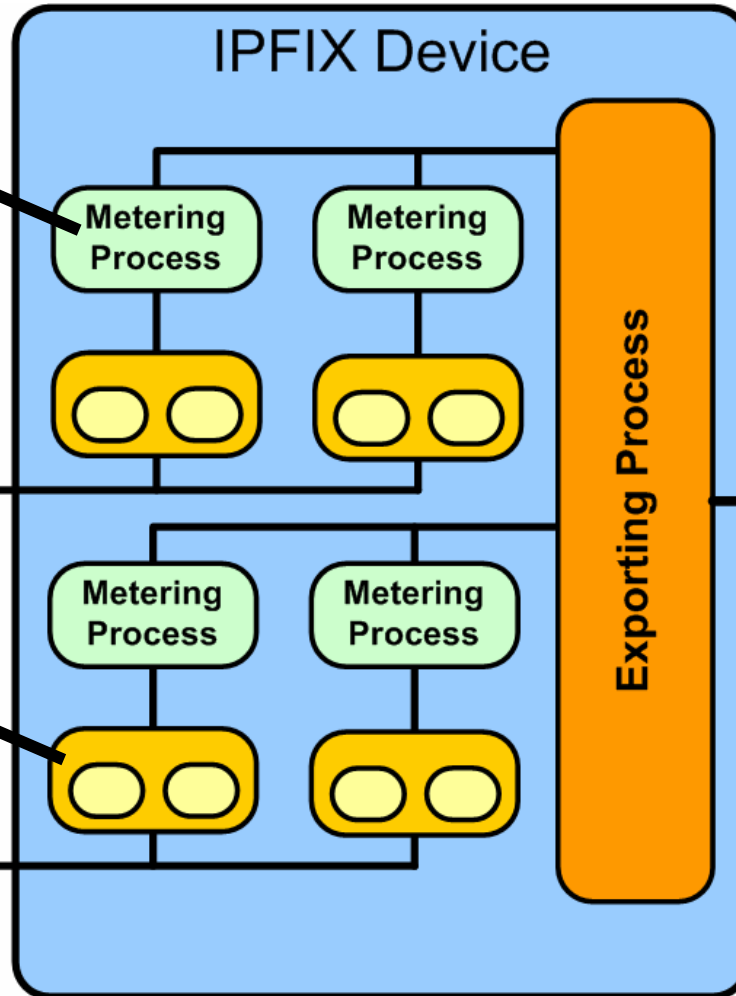
Maintains databases

Maintains statistics



Observation domains

Observation points



Can be push or pull

Can be periodic

Notify for specific events,  
e.g. timeout of a flow or  
arrival of a new flow

Can anonymize traffic

# Reported Flow Properties



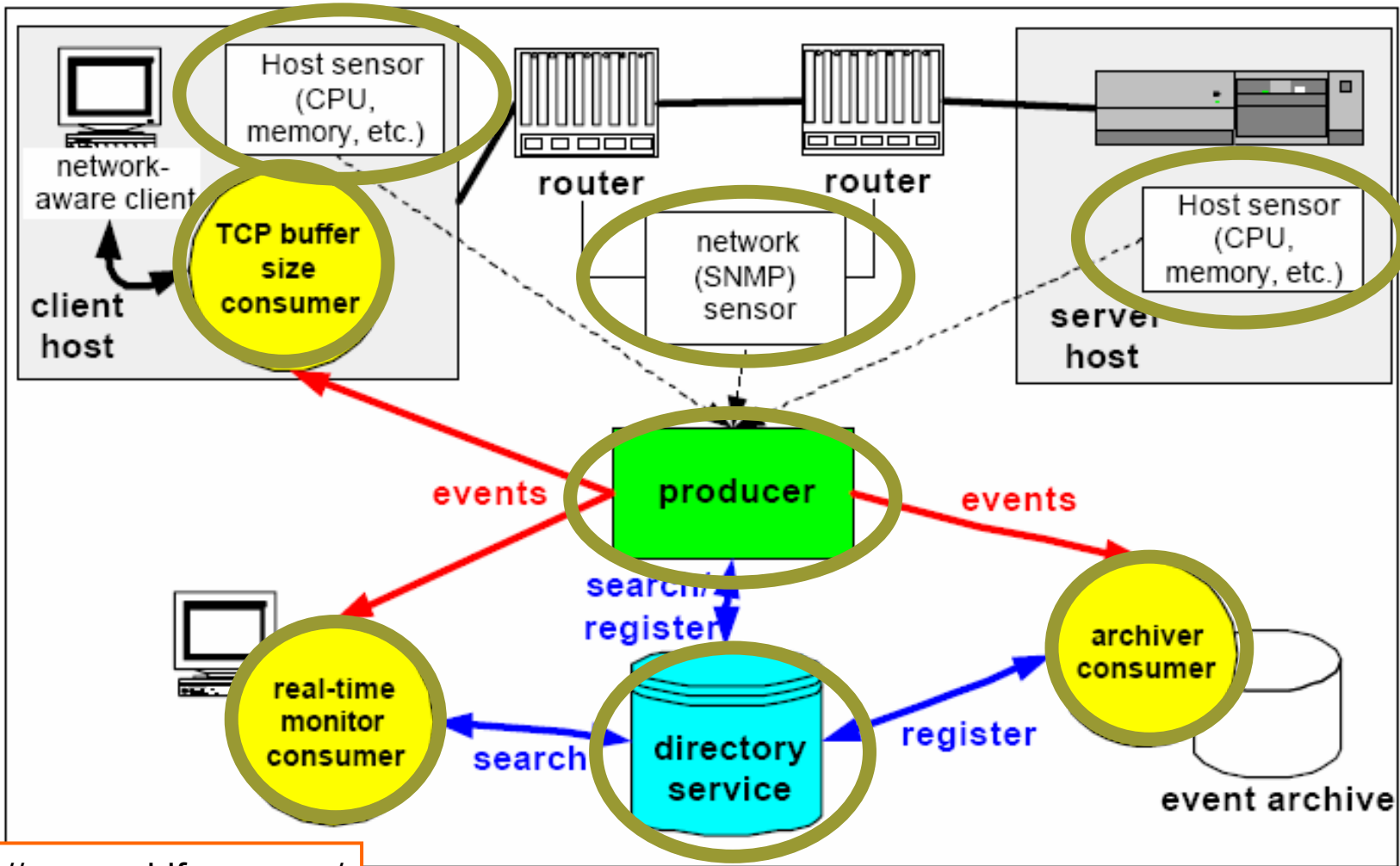
- > IP version number
  - > Source IP address
  - > Destination IP address
  - > Protocol Type
  - > Source port number
  - > Target port number
  - > Packet counter (#)
  - > Byte counter
  - > Type of Service
  - > IPv6 flow label
  - > Top MPLS label
  - > Timestamp of first packet
  - > Timestamp of last packet
  - > Sampling configuration
  - > Observation point identifier
  - > Exporting process identifier
- Must**

- > ICMP type and code
  - > Input interface
  - > Output interface
  - > Multicast replication factor
- Should**

- > TTL
  - > IP header flags
  - > TCP header flags
  - > Dropped packet counter
  - > Fragmented packet counter
  - > Next hop IP address
  - > Source BGP AS number
  - > Destination BGP AS number
  - > Next hop BGP AS number
- May**

- > Access network overview
- > Network monitoring techniques
- > **Monitoring architecture and analysis**
- > Advanced multimedia services
  - IPTV
- > The RTP/RTCP protocol
- > DSLForum
- > Raqmon
- > Conclusion

# Grid Monitoring Architecture (GMA)



<http://www.gridforum.org/>

Source: Global Grid Forum

# Sketch-based change detection



- > Paper: “Sketch-Based Change Detection: Methods, Evaluation and Applications”, B. Krishnamurthy, S. Sen, Y. Zhang and Y. Chen, IMC, 2003
- > Goal: Detect changes in traffic patterns by making sketches of the traffic flows and comparing them to forecast models.
- > Observation: Two ways to identify anomalies:
  - Look for specific patterns
  - Statistics based approach
- > Problem with traditional approach: Only limited amount of time series can be observed
- > Sketch is a probabilistic summary
  - Space efficient
  - Provides probabilistic accuracy
  - Linear (sketches can be combined linearly)

- >  $I = \alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots, \alpha_n$ : Input stream of (key, value) pairs
- >  $\alpha_i = (a_i, u_i)$
- > For every key  $a$  there is a time varying signal  $A[a]$
- > When a data item arrives:  $A[a_i] += u_i$
- > Goal is identifying those signals with a significant change in their behavior
- > We receive input streams at discrete intervals:  $I_1, I_2, I_3, \dots$
- > Ideal case:

- Compute the update for every key  $a$ :

$$O_a(t) = \sum_{i \text{ in } A_a(t)} u_i$$

$\{a_i = a \text{ and } (a_i, u_i) \text{ in } I\}$

- Forecast the value for key  $a$ :  $f_a(t)$

- Compute forecast error for key  $a$ :  $e_a(t) = O_a(t) - f_a(t)$

- Raise alarm if forecast error is to big

Making per key updates and forecasts can be very processing intensive for a large key space

# Sketch-Based Model

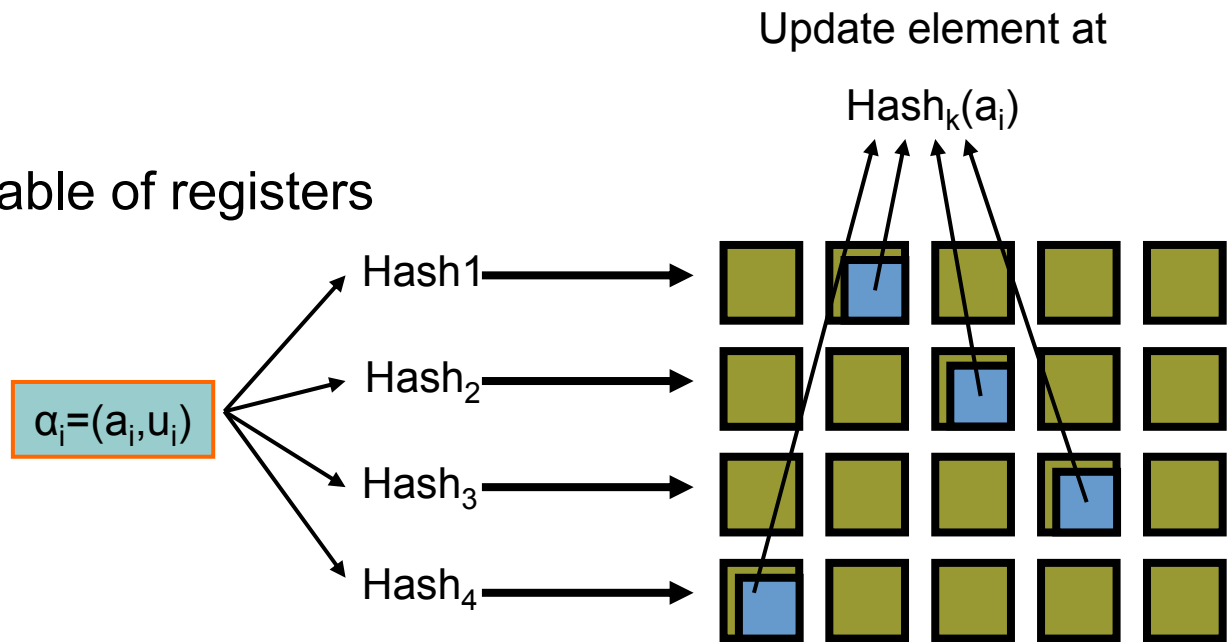
- > Three modules
  - Sketch module (summarizes data in sketch)
  - Forecast module (make forecast of the sketch)
  - Change detection module (determine significant changes )

> 
$$U_a = \sum_{i \text{ in } A_a(t)} u_i$$

> Sketch has  $H \times K$  table of registers

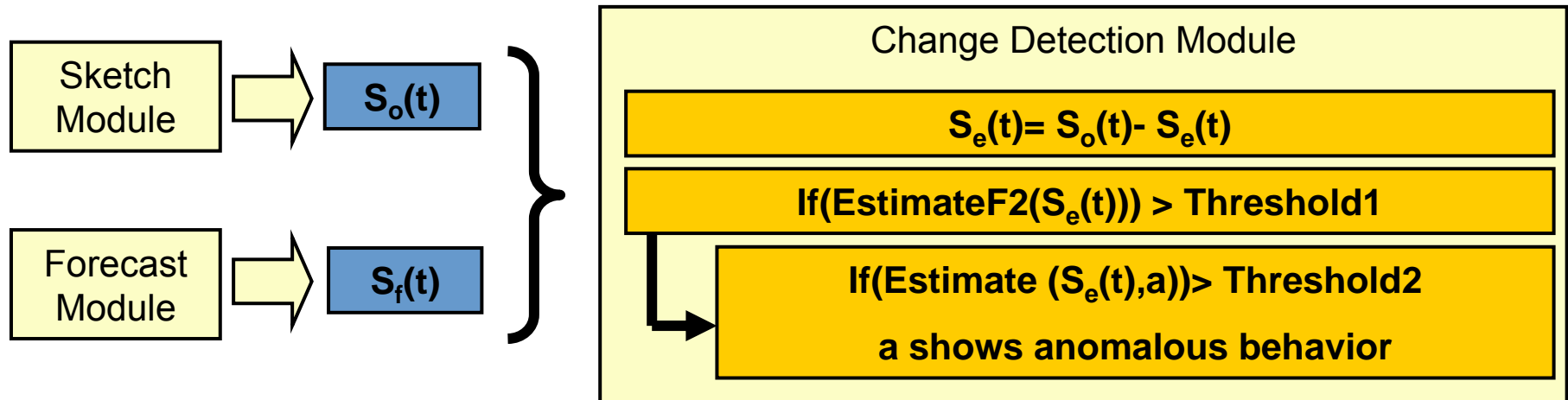
>  $H$  hash functions

$Hash_k: [u] \rightarrow [K]$



# Identifying anomalies

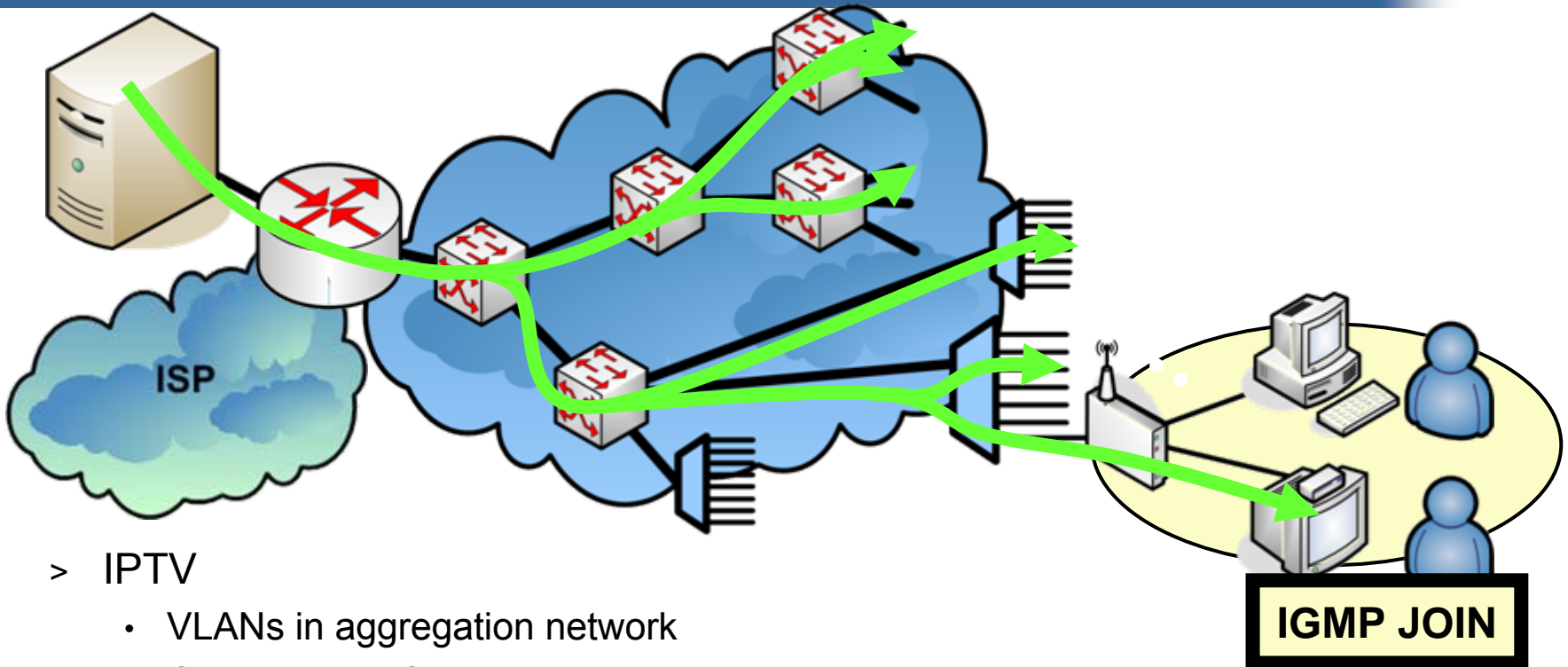
- > Sketch operations:
  - Update(S,a,u): update the sketch structure
  - Estimate(S,a): estimate the value of key a
  - EstimateF2(S): estimate the second moment of the sketch
  - Combine( $c_1, S_1, c_2, S_2, c_3, S_3, \dots$ ): combine a number of sketches linearly
- > Forecast can be made in a number of ways (e.g. moving average)



- > Paper: “What’s New: Finding Significant Differences in Network Data Streams”, G. Cormode and S. Muthukrishnan, Infocom, 2004
- > Goal: Find significantly large differences in traffic, over time, between interfaces and routers. (deltoid)
- > Required properties
  - Small space
  - Small time per update (operate at network line speed)
  - Guaranteed accuracy
- > Mostly, operators are interested in flows that stand out
  - Number of distinct flows on a link
  - Number of tiny flows
  - Heavy hitters
- > Difference can be
  - Absolute, e.g. a big difference in number of packets sent in one hour and the next
  - Relative, e.g. a big ratio of the number of packets sent in one hour and the next
  - Variational, e.g. a large variance of the number of packets sent over multiple hours
- > Look for differences that are a user-specified fraction of the total difference

- > Access network overview
- > Network monitoring techniques
- > Monitoring data analysis
- > **Advanced multimedia services**
  - IPTV
- > The RTP/RTCP protocol
- > DSLForum
- > Raqmon
- > Conclusion

- > Access Network has migrated towards an infrastructure for triple play service delivery
  - VOIP
  - High Speed Internet
  - IPTV



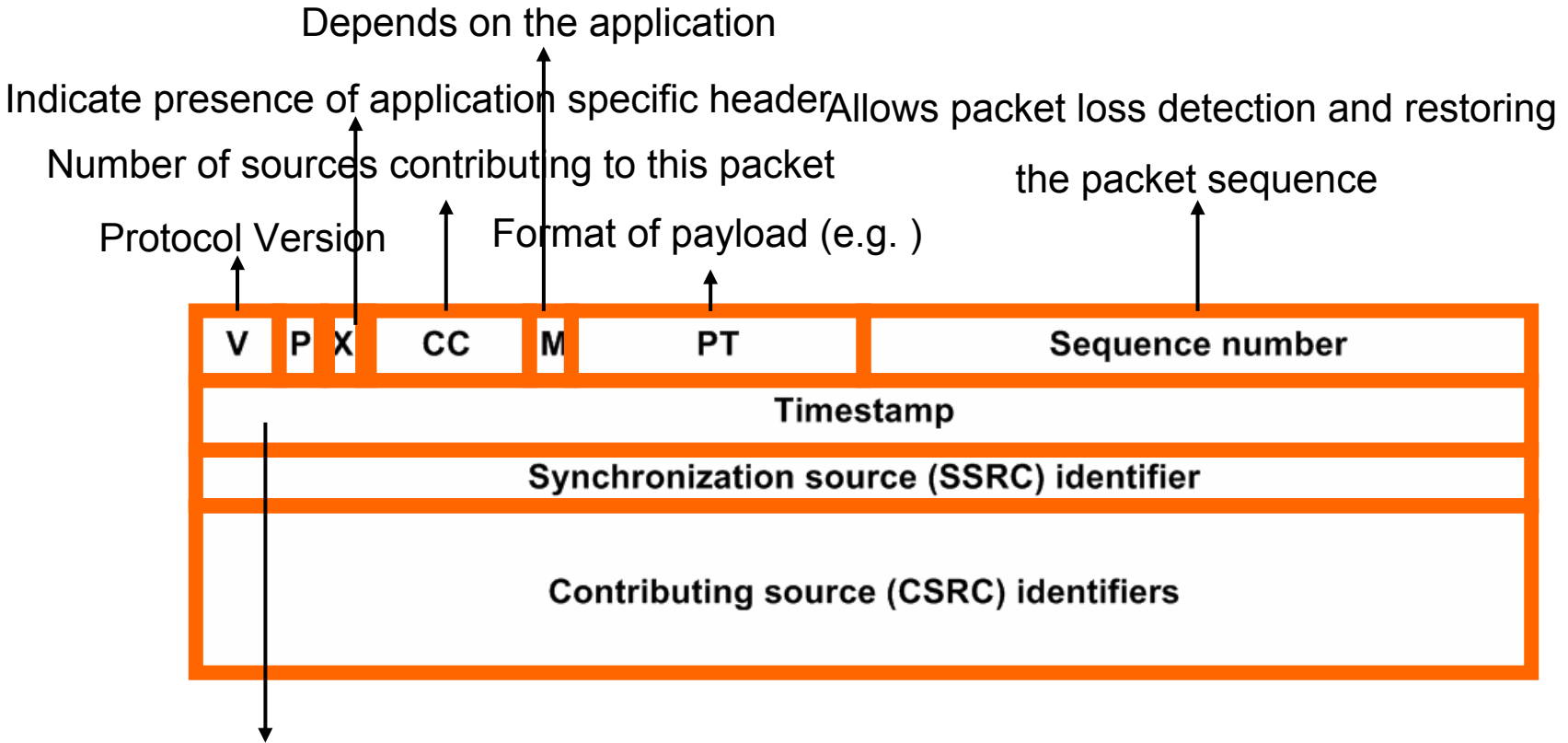
## > IPTV

- VLANs in aggregation network
- Client sends IGMP join message to switch to a channel
- RTP/RTCP is used to carry the video packets over the network
- Access node can snoop/proxy IGMP messages to allow for faster channel switching
- QoE is essential for IPTV

- > Access network overview
- > Network monitoring techniques
- > Monitoring data analysis
- > Advanced multimedia services
  - IPTV
- > **The RTP/RTCP protocol**
- > DSLForum
- > Raqmon
- > Conclusion

- > RFC 3550: “A Transport Protocol for Real-Time Applications”
- > Aimed at real-time applications
  - Audio
  - Video
- > Two protocols:
  - RTP: Real-time Transport Protocol
  - RTCP: RTP Control Protocol
- > Extra functionality:
  - Mixers
  - Translators

# RTP Packets



Sampling instance of first octet of packet:  
Allows for jitter calculation

Communication involving different media will use several RTP/RTCP connections, the different media do not use one stream

Allows synchronized presentation of the data

# RTCP



- > Can be encrypted
- > Packet formats:
  - SDES, source description items
  - BYE, end of participation
  - APP, application specific
  - SR, Sender Report
  - RR, Receiver Report
- > RTCP packets are concatenated in compound RTCP packets

Encryption Prefix	RR/SR	SDES	APP/BYE
-------------------	-------	------	---------

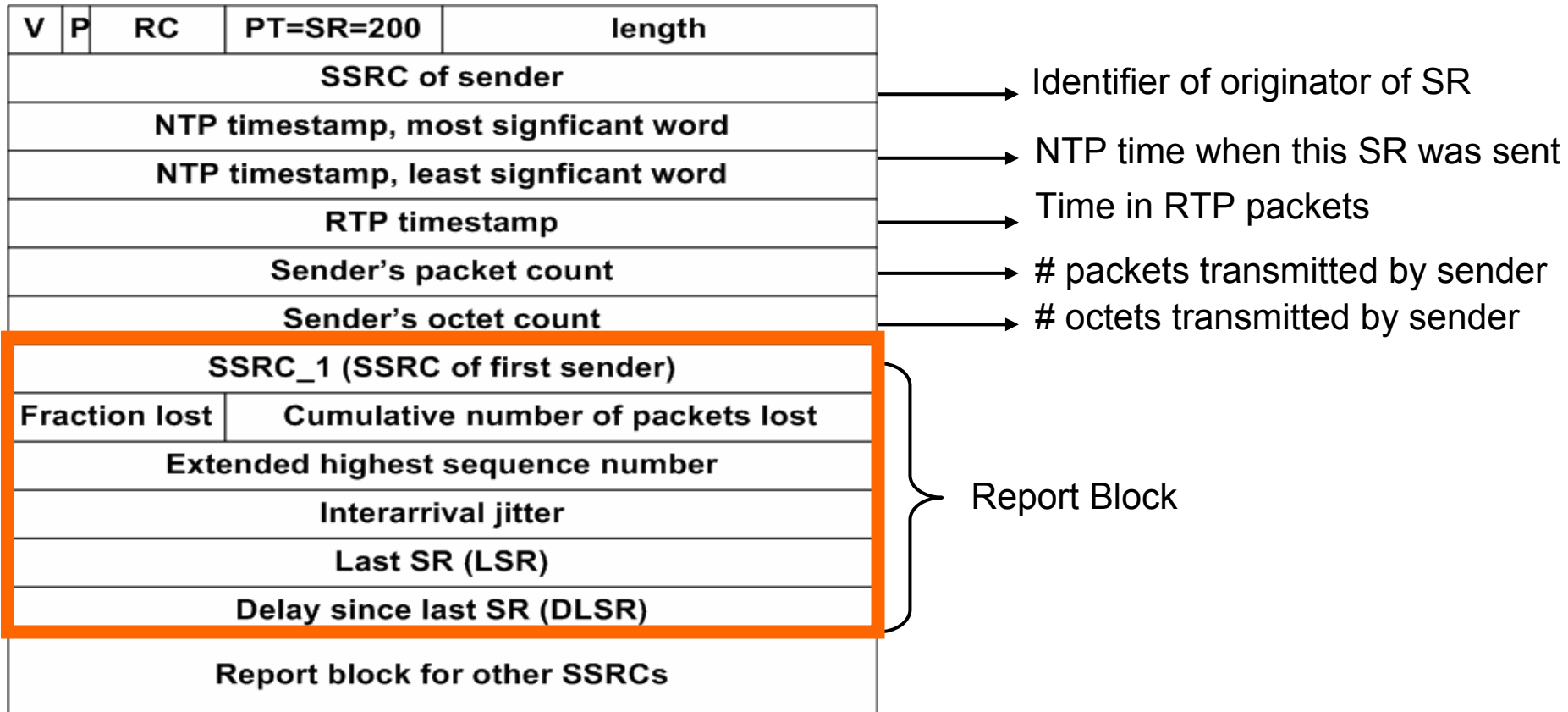
- > The bandwidth that is used for reporting is adapted to the number of participants
- > Bandwidth used for reporting: 5% of application bandwidth
- > Minimal interval between the sending of reports: 5 sec

# Reports



Sender Report

Number of report blocks



# Report Blocks



V	P	RC	PT=SR=200	length
SSRC of sender				
SSRC_1 (SSRC of first sender)				
Fraction lost		Cumulative number of packets lost		
Extended highest sequence number				
Interarrival jitter				
Last SR (LSR)				
Delay since last SR (DLSR)				
Report block for other SSRCs				

## Loss information:

- Fraction of packets that the client did not receive
- Total number of packets the client did not receive
- Highest sequence number received up to this moment

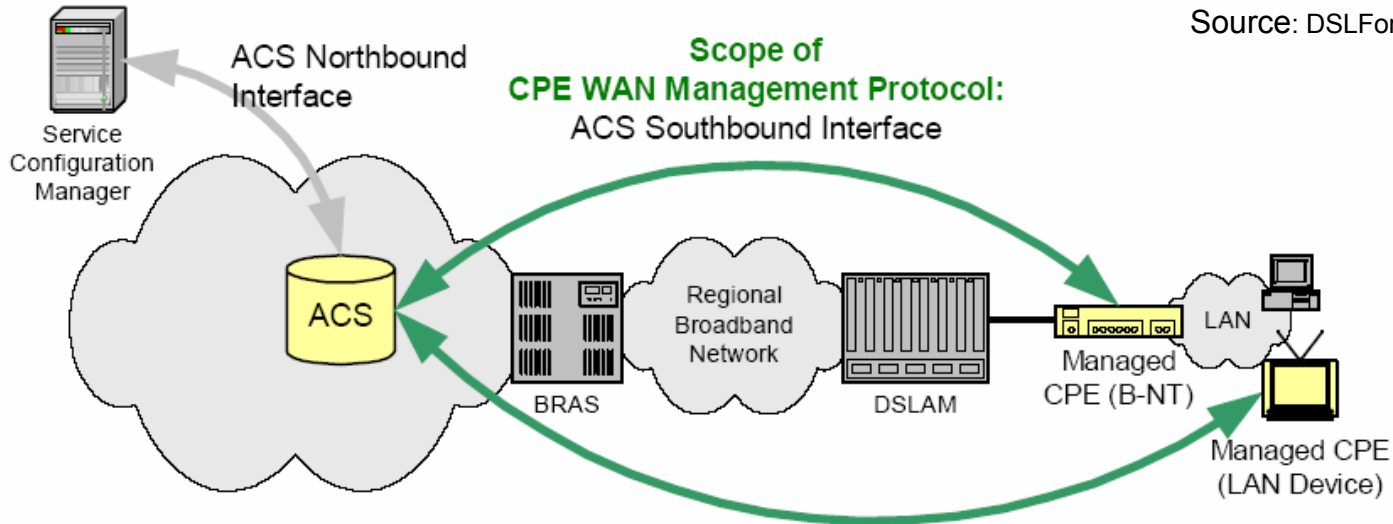
**Jitter information:** Interarrival jitter of packets

**Delay information:** Allows server to calculate RTT

Important tools for QoE monitoring

- > Access network overview
- > Network monitoring techniques
- > Monitoring data analysis
- > Advanced multimedia services
  - IPTV
- > The RTP/RTCP protocol
- > **DSLForum**
- > Raqmon
- > Conclusion

- > [www.dslforum.org](http://www.dslforum.org)
- > “DSL Forum is a consortium of approximately 200 leading industry players covering telecommunications, equipment, computing, networking and service provider companies” www.dslforum.org
- > TR-069: Communication between customer premises equipment (CPE) and an auto configuration server (ACS)
- > Extend the reach of a management platform to devices in the home network
- > Goals:
  - Auto configuration and dynamic service provisioning
  - Software/firmware image management
  - Status and performance monitoring
  - Diagnostics

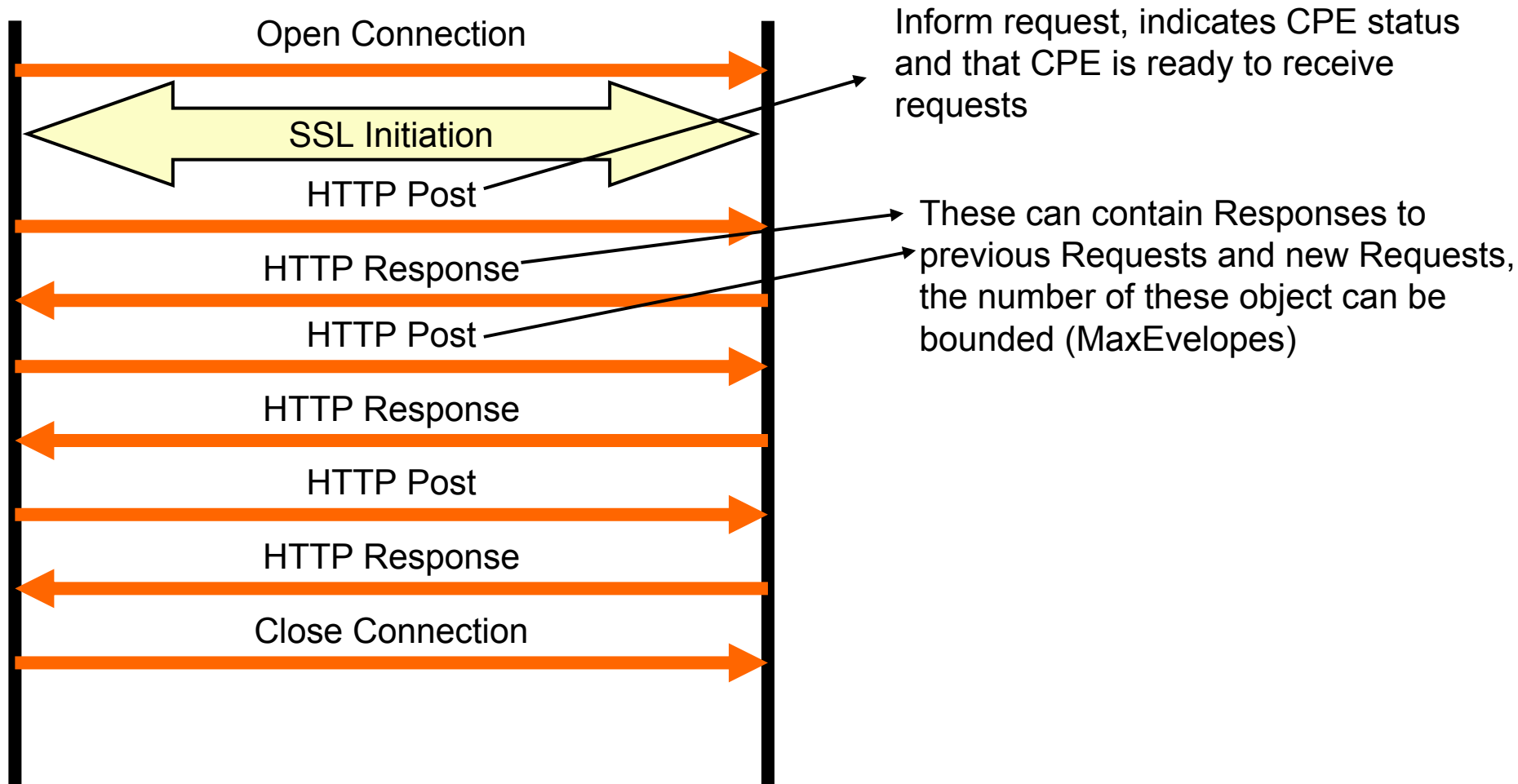


- > Managed device can be different types of home equipment
  - Set top box
  - Residential gateway
  - Game console
  - VOIP device

- > Security is essential in providing the management functionality that is provided by TR-069
- > NAT and firewall
- > TR-069 provides a protocol to manage remote devices from an auto configuration server (ACS)
- > Read and write parameters to configure CPE and monitor CPE statistics
- > Notification from CPE to its ACS
- > ACS discovery:
  - DNS
  - DHCP option
  - Default URL

CPE/ACS Application
RPC
SOAP
HTTP
SSL/TLS
TCP/IP

# Operations



# RPC Methods



- > GetRPCMethods
  - > SetParameterValues
  - > GetParameterValues
  - > GetParameterNames
  - > SetParameterAttributes
  - > GetParameterAttributes
  - > AddObject
  - > DeleteObject
  - > Reboot
  - > Download
  - > Upload
  - > FactoryReset
  - > GetQueuedTransfers
  - > ScheduleInform
  - > SetVouchers
  - > GetOptions
- > GetRPCMethods
  - > Inform
  - > TransferComplete
  - > RequestDownload
  - > Kicked

Optional

Required

- > Object models with parameters are defined in other TRs e.g.
  - TR-069: Internet Gateway Device
  - TR-098: Internet Gateway Device 1.1
  - TR-104: VOIP CPE Device
  - TR-106: TR-069 Enabled Device
  - WT-135: Set top box
  - WT-107: Internet Gateway Device 2
- > TR-069 extentions:
  - TR-111: NAT & Firewall traversal

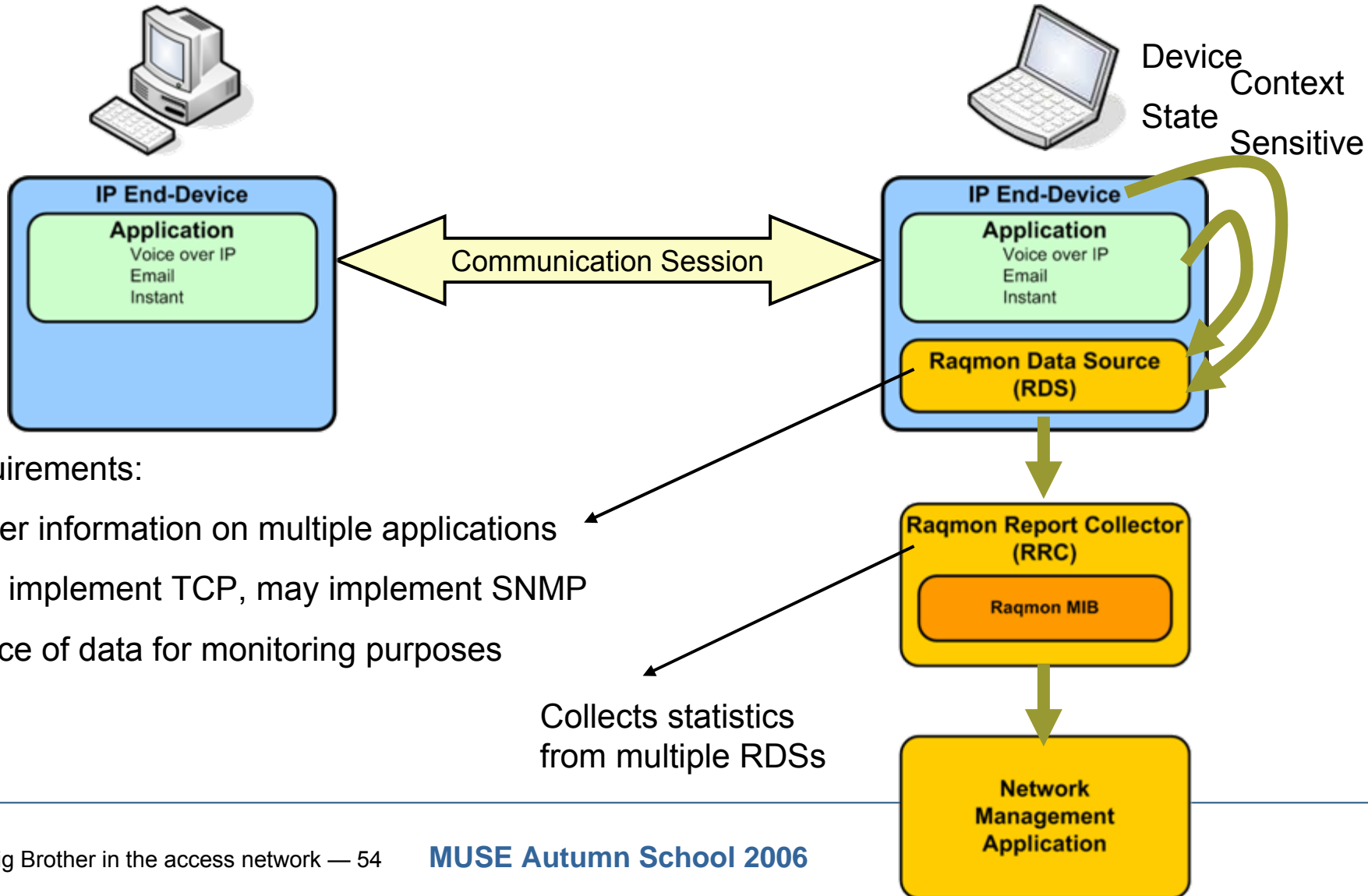
- > Object models allow to retrieve parameters related to QoE:
  - InternetGatewayDevice.IPPingDiagnostics: Allow access to an IP-layer ping test
  - InternetGatewayDevice.LANDevice.{i}.LAN-EthernetInterfaceConfig.{i}.Stats: Statistics on packets/bytes that have been sent/received on LAN interface
  - InternetGatewayDevice.LANDevice.{i}.WLAN-Configuration.{i}: Information on the wireless interface of the device, e.g. maxbitrate, the number of wireless channels that is currently in use
  - InternetGatewayDevice.WANDevice.{i}.WAN-CommonInterfaceConfig: Information on the WAN interface (e.g. For DSL, Ethernet, POTS,...)
  - InternetGatewayDevice.WANDevice.{i}.WAN-DSLInterfaceConfig: Information on the DSL line
  - InternetGatewayDevice.WANDevice.{i}.WAN-DSLiagnostics: Diagnostics information on the DSL line
  - ...

- > Access network overview
- > Network monitoring techniques
- > Monitoring data analysis
- > Advanced multimedia services
  - IPTV
- > The RTP/RTCP protocol
- > DSLForum
- > **Ragmon**
- > Conclusion

- > Real-time Application QoS Monitoring Framework
- > Developed by the rmonmib working group of the IETF
- > Internet drafts:
  - draft-ietf-rmonmib-raqmon-framework-16
  - draft-ietf-rmonmib-raqmon-pdu-14
  - draft-ietf-rmonmib-raqmon-mib-12
- > Allow end devices and applications to report QoS statistics in real time
- > Allows reporting on a variety of statistics
- > Example: VOIP call QoE depends on:
  - Call setup time
  - Media related performance metrics
  - Type of codec
  - Network resources
  - End device resources

- > The Real Time Application QoS Monitoring (RAQMON) Framework offers a mechanism to report the end-to-end QoS experience appropriate for a specific application context by providing mechanisms to report a subset of metrics from a pre-defined list.
- > Correlates statistics that involve:
  - “user/session/application” parameters: e.g. session setup, session duration
  - “IP end device” parameters: e.g. CPU usage, memory usage
  - “Transport Network” parameters: e.g. delay, jitter, packet loss
- > Framework:
  - Set of basic metrics to report
  - Requirements for underlying transport protocols
  - Extension of RMON Management Information Base

# Raqmon Architecture



Requirements:

Gather information on multiple applications

Must implement TCP, may implement SNMP

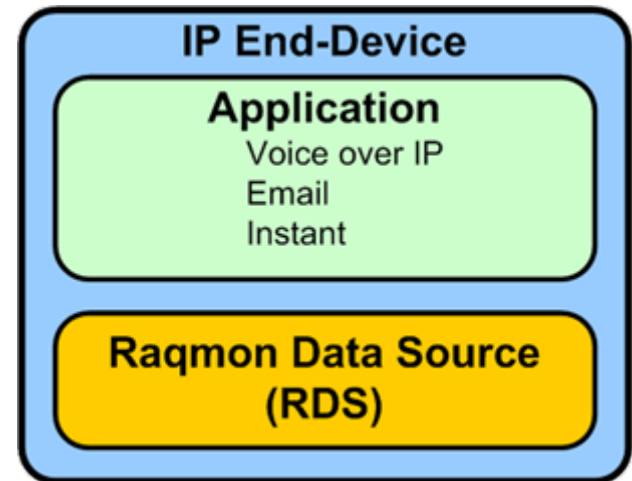
Source of data for monitoring purposes

Collects statistics from multiple RDSs

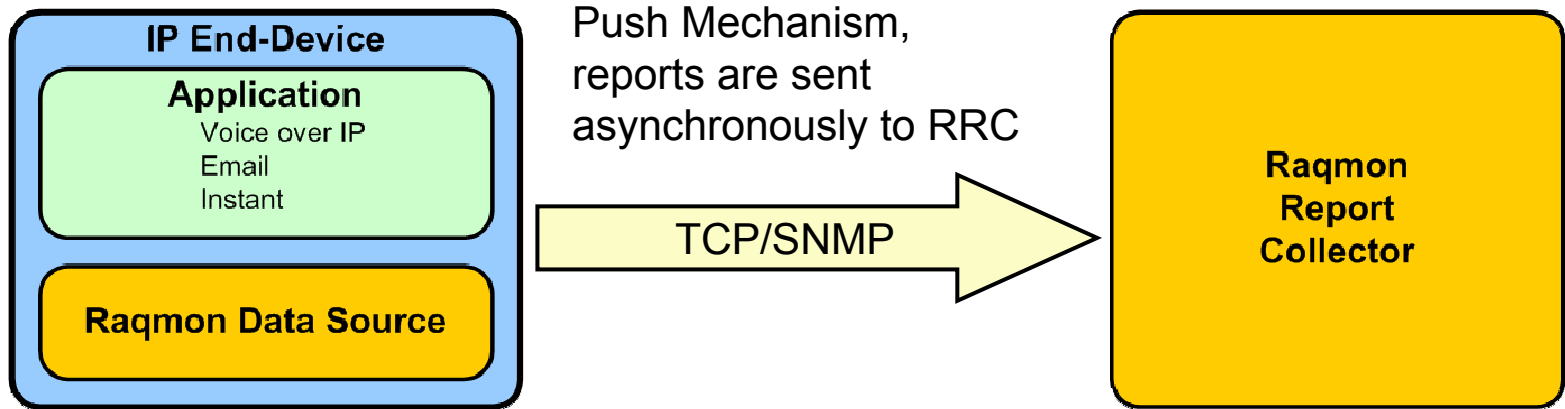
# Raqmon Data Source



- > Requirements:
  - Gathers information on multiple applications
  - Must implement TCP, may implement SNMP
- > Configurable parameters:
  - Time interval between PDUs
  - IP address of RRC



# Raqmon RDS – RRC communication



## RAQMON Protocol Data Unit

### Basic part

- entries from predefined list of QoS parameters
- as perceived by end-device

### Application specific extensions

- vendor-, equipment-, device-specific
- owner of definition indicated by SMI-number

Identification using  
DSRC field  
(Data Source identifier)

Scalability: no more than 10 % of network bandwidth should be used for RDS/RRC reporting

# Raqmon PDU Basic parameters

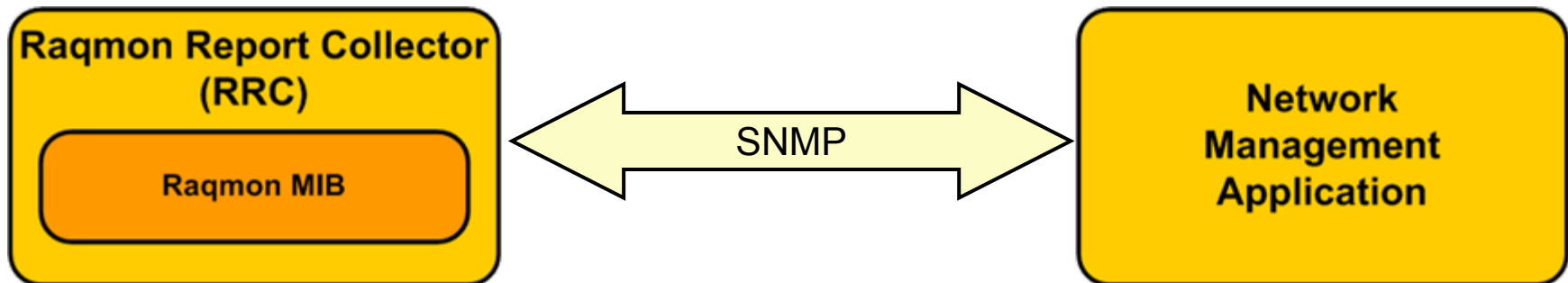


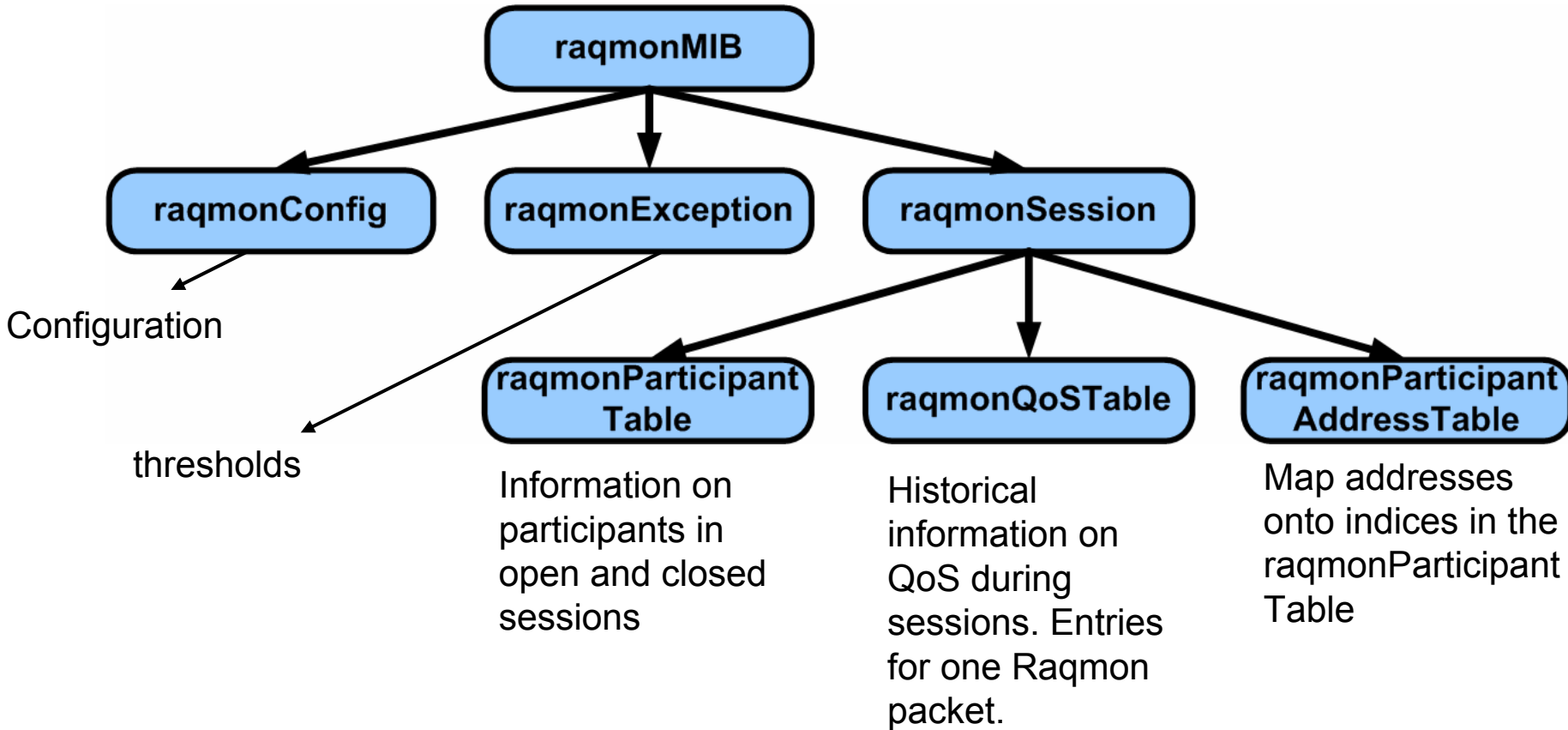
- > Data source address
- > Receiver address
- > Data source name
- > Receiver name
- > Data Source Device Port Used
- > Receiver Device Port Used
- > Session Setup Date/Time
- > Session Setup Delay
- > Session Duration
- > Session Setup Status
- > Round Trip End-to-End Network Delay
- > One Way End-to-End Network Delay
- > Application Delay
- > Inter-Arrival Jitter
- > IP Packet Delay Variation
- > Total Number of Application Packets Received
- > Total Number of Application Packets Sent
- > Total number of Application Octets Received
- > Total number of Application Octets Sent
- > Cumulative Packet Loss
- > Packet loss in Fraction
- > Cumulative Application Packet Discards
- > Packet Discards in Fraction
- > Source Payload Type
- > Receiver Payload Type
- > Source Layer 2 Priority
- > Source TOS/DSCP Value
- > Destination Layer 2 Priority
- > Destination TOS/DSCP Value
- > CPU Utilization in Fraction
- > Memory Utilization in Fraction
- > Application Name/version

# Raqmon Resource Collector



- > Receives Raqmon PDUs
- > Analyze and stores PDU information in Raqmon MIB
- > Management platform communicates with RRC using SNMP
- > Computationally resourceful
- > Provides storage and aggregation point for multiple RDS
- > RDS – RRC: not a one to one mapping,
- > RRC is able to perform aggregation and statistical operations this results in min/max/mean values





- > Network and services have changed
- > QoE is of prime importance for the new services
- > Monitoring is becoming more and more a part of the access network
- > Broad domain, including:
  - Monitoring the devices
  - Monitoring the applications
  - Service specific monitoring techniques
  - Analyzing monitor information and detecting problems
  - Extend reach of the management platform to the home network