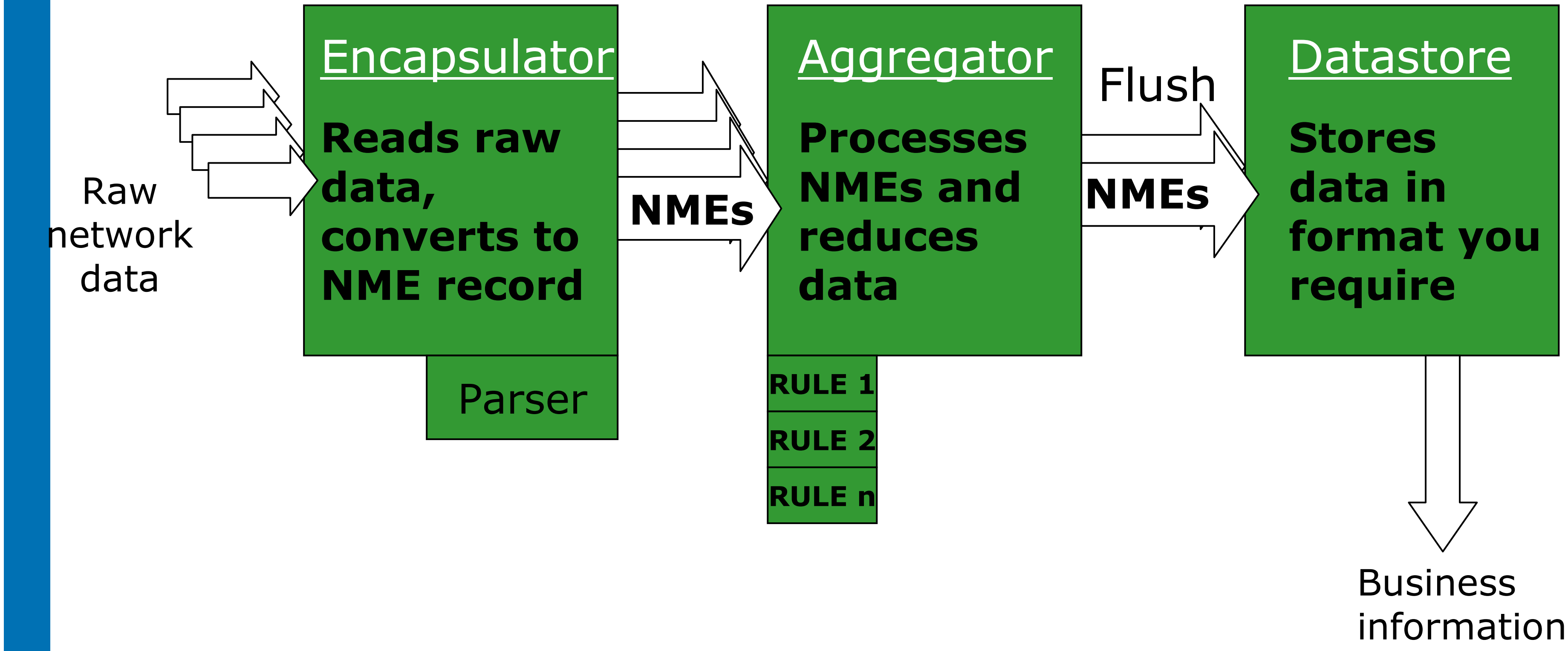
HP IUM Fundamentals

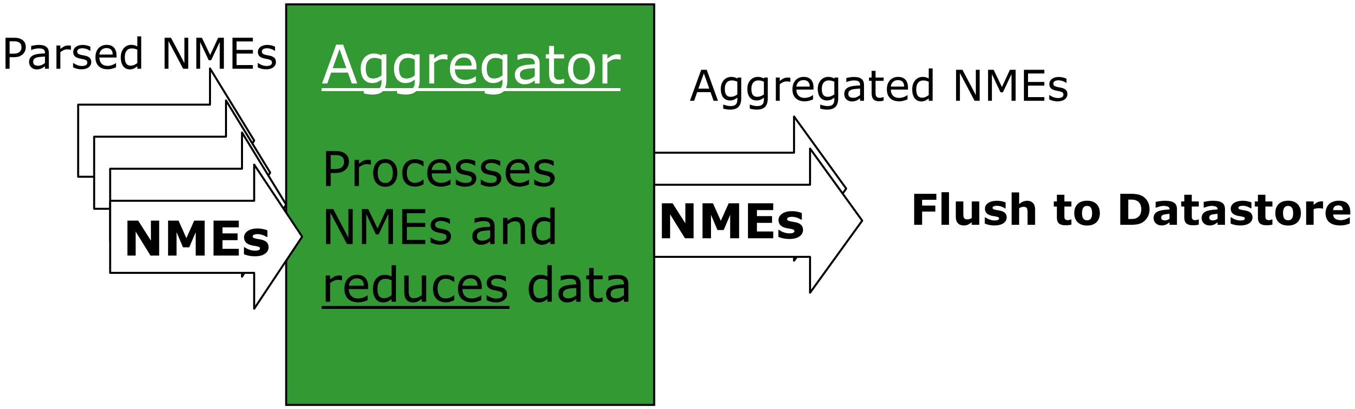
Aggregators & Datastores
IUM Deployment

IUM Components - Aggregator



IUM Components - Aggregator

- The Aggregator reduces data (NMEs)
- Reduces data using Aggregation Schemes. Each Scheme has a set of Rules
- Rules form a Rule Chain
- Aggregation is done in memory
- Reduced Data (NMEs) are Flushed to the Datastore periodically



IUM Components - Aggregator

- Rules are used to construct **Aggregation Schemes**. The rules control how an **Aggregation Tree** is constructed (nodes and branches) and how NMEs are manipulated and stored as they pass through the Tree.
- The **leaf nodes** of the Tree are typically aggregated NMEs ready to be **flushed** to the **datastore**.
- Rules are linked together in a sequence as **Rule Chains**.
- There can be a number of Rule Chains in a Scheme.
- Aggregation Schemes reside in the Aggregator.
- The Aggregator builds an Aggregation Tree in **memory** and stores the NMEs in the Aggregation Tree.

IUM Components - Aggregator

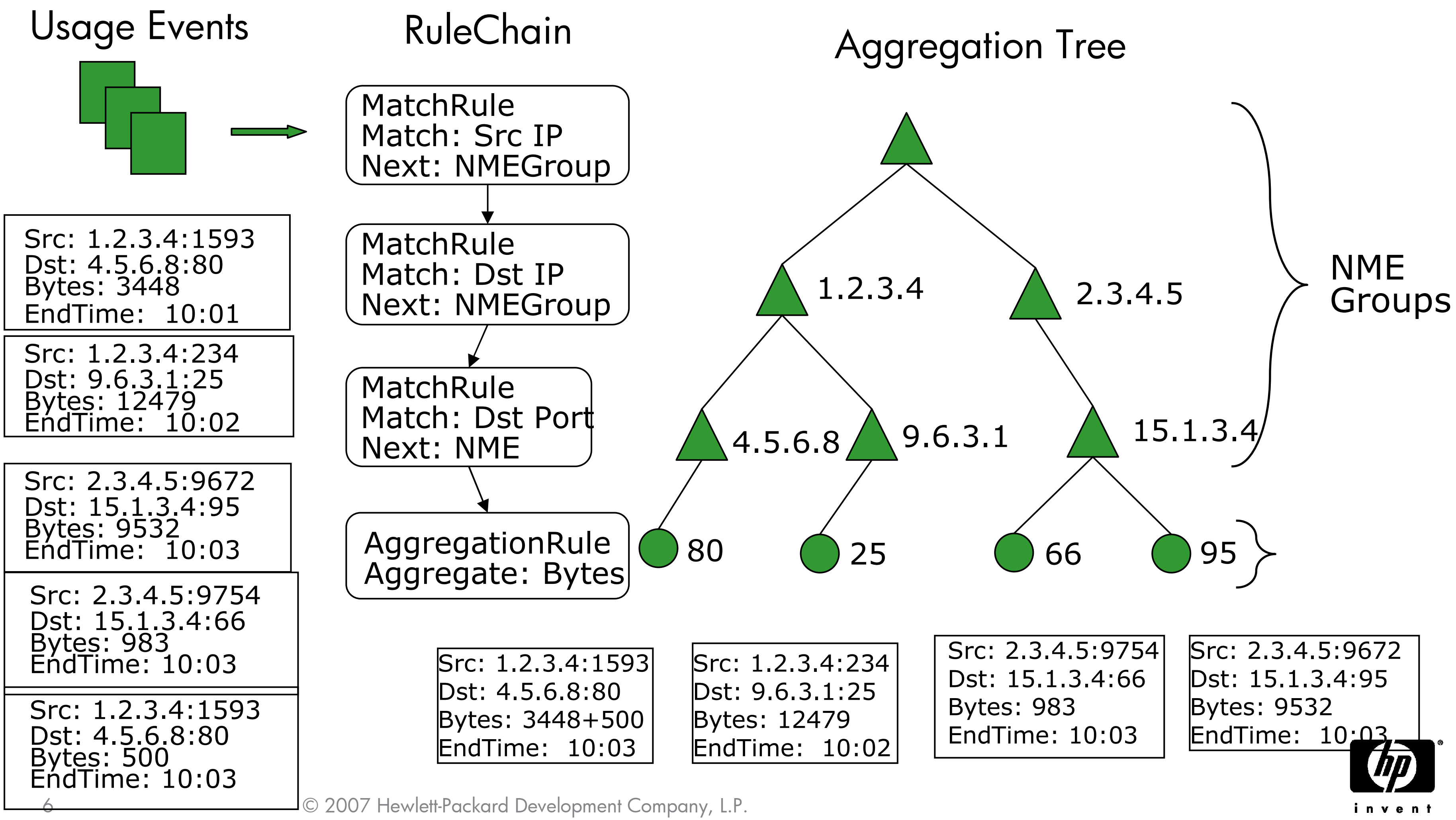
There are a number of different Aggregation Rules:

- AdornmentRule
- AggregationRule
- ConditionalRule
- ConditionRangeRule
- CorrelatorMatchRule
- DNSLookupRule
- FilterRule.
- HashMatchRule
- HistogramMatchRule
- JNDILookupRule
- ProxyURLRule.
- RangeCorrelatorMatchRule
- SessionMatchRule
- SimpleSessionState
- Split NMERule
- SplitURLRule
- StoreRule
- VectorMatchRule

(For full details of each rule see the Collector Component Reference)

IUM Components - Aggregator

- Example of Aggregation and the Aggregation Tree



Usage Events

Src: 1.2.3.4:1593
Dst: 4.5.6.8:80
Bytes: 3448
EndTime: 10:01

Src: 1.2.3.4:234
Dst: 9.6.3.1:25
Bytes: 12479
EndTime: 10:02

Src: 2.3.4.5:9672
Dst: 15.1.3.4:95
Bytes: 9532
EndTime: 10:03

Src: 2.3.4.5:9754
Dst: 15.1.3.4:66
Bytes: 983
EndTime: 10:03

Src: 1.2.3.4:1593
Dst: 4.5.6.8:80
Bytes: 500
EndTime: 10:03

RuleChain

MatchRule
Match: Src IP
Next: NMEGroup

MatchRule
Match: Dst IP
Next: NMEGroup

MatchRule
Match: Dst Port
Next: NME

AggregationRule
Aggregate: Bytes

Aggregation Tree

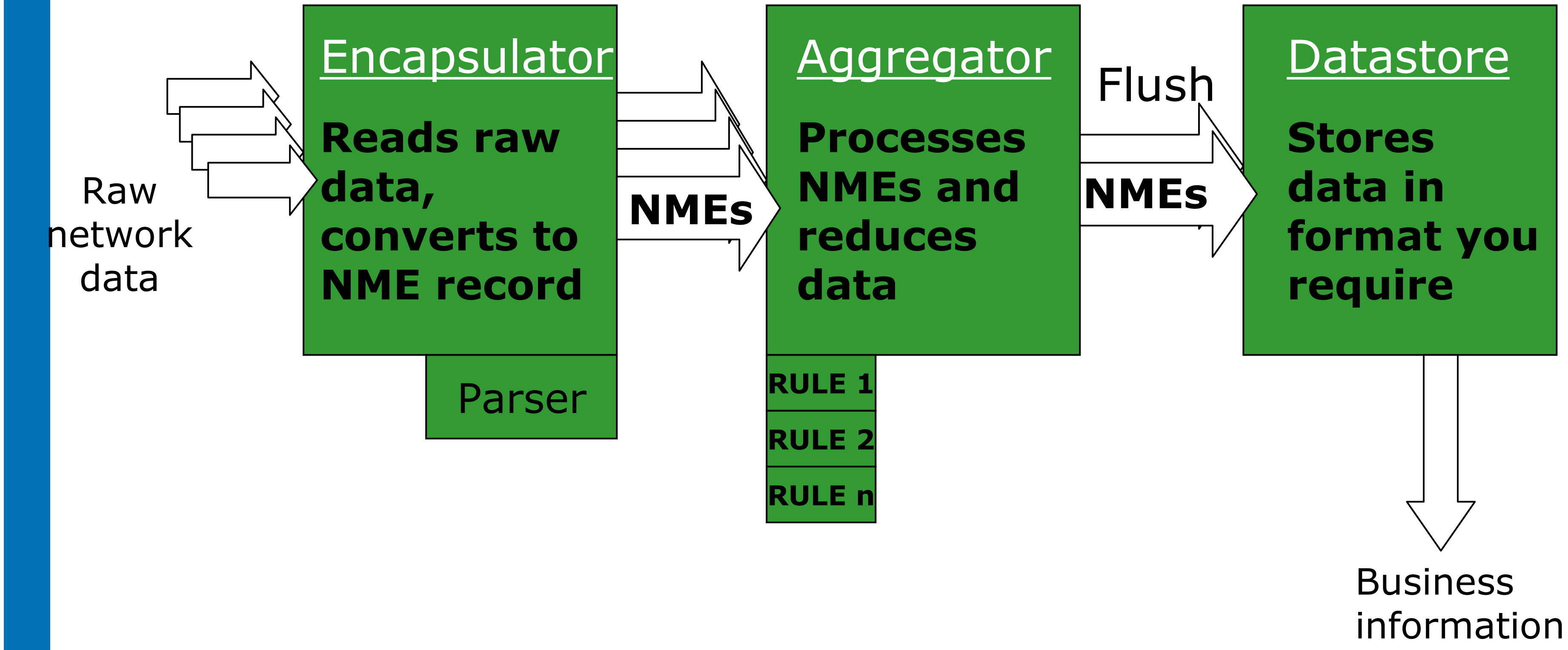
Src: 1.2.3.4:1593
Dst: 4.5.6.8:80
Bytes: 3448+500
EndTime: 10:03

Src: 1.2.3.4:234
Dst: 9.6.3.1:25
Bytes: 12479
EndTime: 10:02

Src: 2.3.4.5:9754
Dst: 15.1.3.4:66
Bytes: 983
EndTime: 10:03

Src: 2.3.4.5:9672
Dst: 15.1.3.4:95
Bytes: 9532
EndTime: 10:03

IUM Components - Datastore



Raw network data

Encapsulator

Reads raw data, converts to NME record

Parser

NMEs

Aggregator

Processes NMEs and reduces data

RULE 1

RULE 2

RULE n

Flush

NMEs

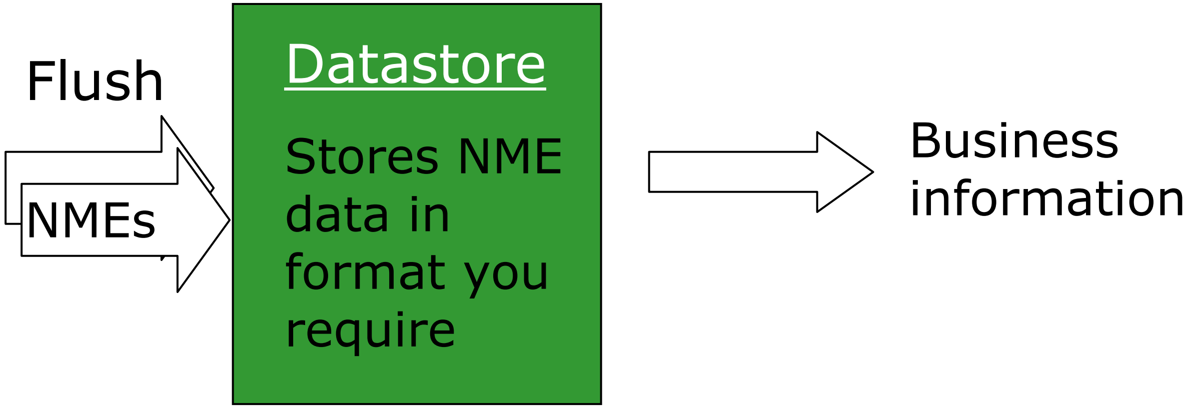
Datastore

Stores data in format you require

Business information

IUM Components - Datastore

- Provides persistent storage of NMEs, flushed from aggregation in memory
- Stores collector state information used during crash recovery
- Support querying facility



Flush

NMEs

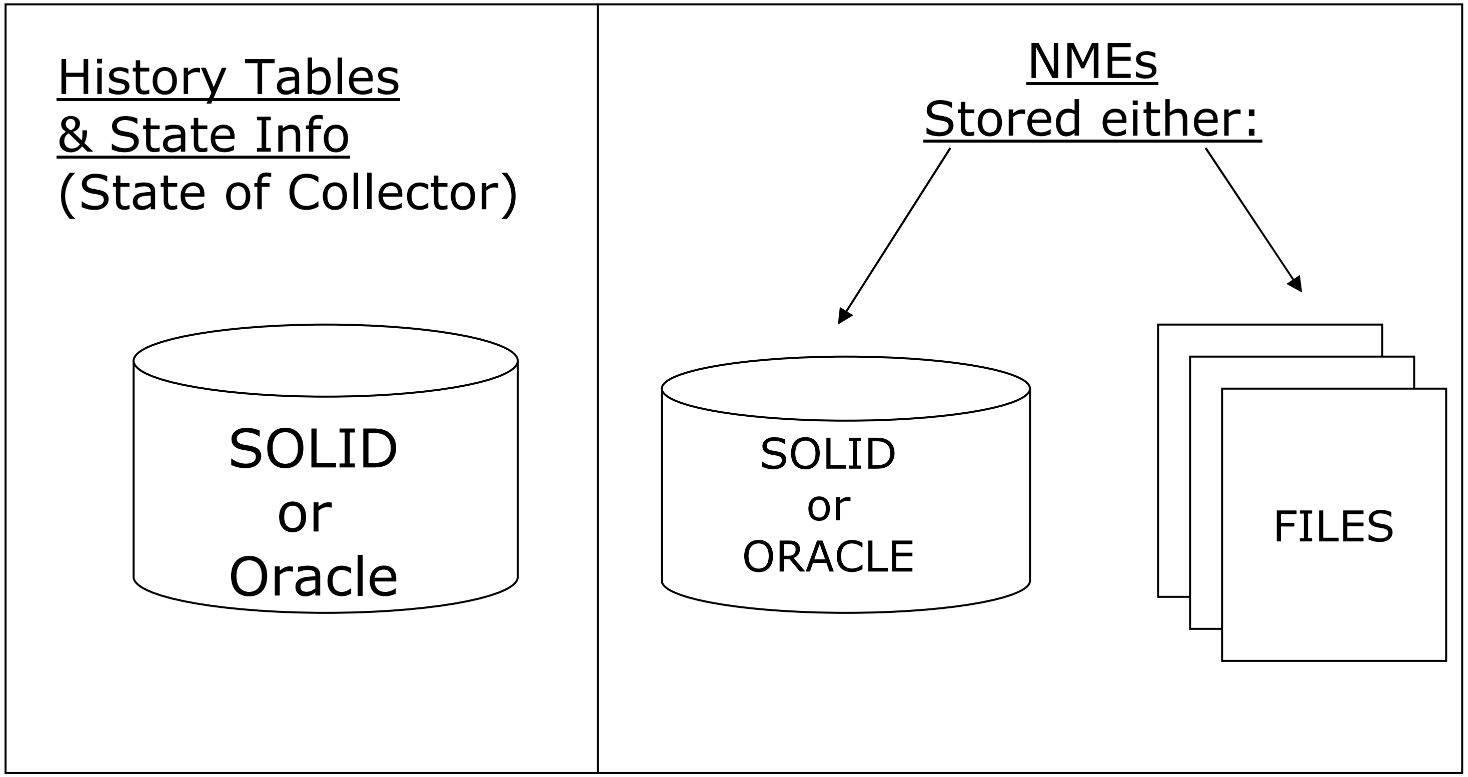
Datastore

Stores NME data in format you require

Business information

IUM Components - Datastore

Every collector has its own datastore



IUM Components - Datastore

- There exist several Datastore components you can configure
- You should select the Datastore driver based on the output data you require (format, destination, quantity, etc.)
  - JDBCDatastore → Stores NME and Metadata in a database
  - FileJDBCDatastore → Stores NMEs as binary files and Metadata stored in database (Solid or Oracle)
  - IDRJDBCDatastore → Stores NMEs in IDR+ format in ASCII files (HTML, XML Tables, Delimited, Configured)
  - ExternalJDBCDatastore → Stores NMEs in a database (per users, table and column definition)
  - ApplicationJDBCDatastore → allows SDK developers to create new plug-ins (like billing apps or other APIs)

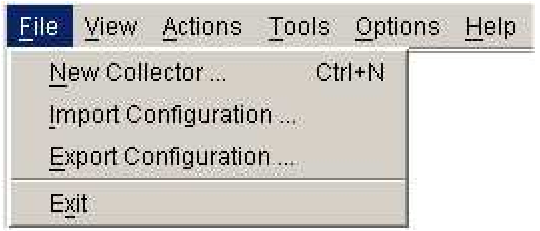
NOTE: To increase performance, tipically select a binary files datastore for your collectors

IUM Deployment – Creating Collectors

- In Launchpad:

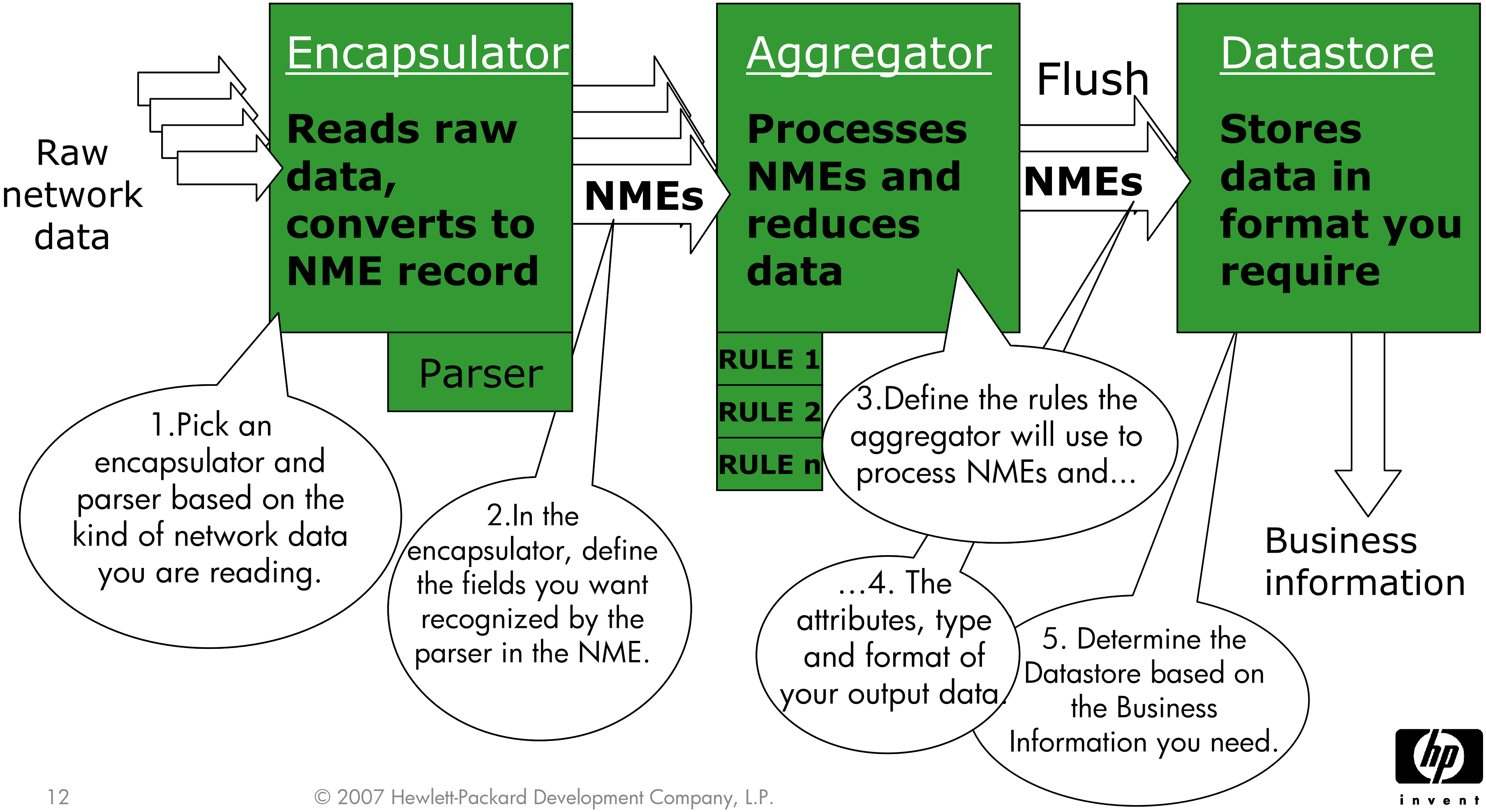
- From the "File" Menu : New Collector (Ctrl+N)

- This command opens a window that allows you to create a collector using custom or factory templates.



IUM Deployment – Creating Collectors

- Steps to build a Collector



1.Pick an encapsulator and parser based on the kind of network data you are reading.

2.In the encapsulator, define the fields you want recognized by the parser in the NME.

3.Define the rules the aggregator will use to process NMEs and…

…4. The attributes, type and format of your output data.

5. Determine the Datastore based on the Business Information you need.

IUM Deployment – Creating Collectors

- The Wizard allows you to select the following Pre-configured Encapsulators:

Apache WEB (ASCII)
Cisco–DHCP (ASCII)
Cisco IP Acct (Poll) *
Cisco Netflow (ASCII, continous)
Cisco Netflow (ASCII, directory)
Cisco Netflow (ASCII, single file)
Cisco Netflow (Demo)
Cisco Netflow (UDP)
Cisco Netflow v1(UDP)
Cisco Netflow V5 (UDP)
Cisco Netflow V7 (UDP)

Cisco Netflow V8 RouterAS Flow Record
Cisco Netflow V8 RouterDstPrefix Flow Record
Cisco Netflow V8 RouterPrefix Flow Record
Cisco NetflowV8 RouterProto Flow Record
Cisco Netflow V8 RouterSrcPrefix Flow Record
Cisco RTT MIB Encapsulator (poll) *
Cisco WANATM
Collector (poll) *
Collector (poll, session)**
Demo Encapsulator
Generic CLF Proxy (ASCII)

IUM Deployment – Creating Collectors

Generic CLF Web (ASCII)

Intermail (ASCII)

LucentLivingstonPortMasterRadius

MS-DHCP (ASCII)

MS-Netflow(ASCII)

MSIISFTP (ASCII)

MSIISWeb (ASCII)

Netscape Enterprise/Fasttrack Server

Netscape Proxy CLF (ASCII)

Netscape Proxy Extended CLF (ASCII)

PortalInfranetRadius (ASCII)

PresideRadius (ASCII)

Radius (ASCII)

RMON2 Encapsulator (poll) *

SMD (Unix)

SNMP Encapsulator (poll) *

SNMP Encapsulator Table (poll) *

Squid (ASCII)

Session (Addr Range)

Session (Single Addr)

StarVox VPN

Web (ASCII)

WU-FTP (ASCII)

ZeusWeb (ASCII)

IUM Deployment – Creating Collectors

- The Wizard allows you to select the following Pre-configured Aggregation Schemes:

Aggregation (Addr Range)

Aggregation (CiscoNFV8RouterAS)

Aggregation (CiscoNFV8RouterDstPrefix)

Aggregation (CiscoNFV8RouterPrefix)

Aggregation (CiscoNFV8RouterProtoPort)

Aggregation (CiscoBFV8RouterSrcPrefix)

Aggregation (Cisco-DHCP)

Aggregation (CiscoWANATM)

Aggregation (Demo FTP)

Aggregation (Demo web)

Aggregation (Demo WU-FTP)

Aggregation (Demo Radius)

Aggregation (InterMail)

Aggregation (LucentLivingstonPortMaster)

Aggregation (MS-DHCP)

Aggregation (MS-Netflow)

Aggregation (ProxyCLF)

Aggregation (Proxy Extended CLF)

Aggregation (Radius)

Aggregation (SMD)

IUM Deployment – Creating Collectors

Aggregation (Single Addr)

Aggregation (Squid)

Aggregation (StarVox VPN)

Aggregation (Web)

Correlation (Addr Range)

Correlation (Single Addr)

Histogram

No aggregation

No aggregation (Cisco RTT MIB)

No aggregation (RMON2)

No aggregation (SNMP)

Src Dst IP (Netflow fields)

Src Dst IP (simple)

Src Dst IP (sorted)

IUM Deployment – Creating Collectors

- The Wizard allows you to select the following Pre-configured Aggregation Schemes:

  - Accumulating Binary File Datastore
  - Application Datastore
  - Binary File (DDS)
  - Database (DDS)
  - Delimiter Seperated (IDR+)
  - External Database
  - Fixed Width (IDR+)
  - HTML (IDR+)
  - IPDR (IDR+)
  - Oracle Database (DDS)
  - TAPS Fixed Width (IDR+)
  - XML (IDR+)

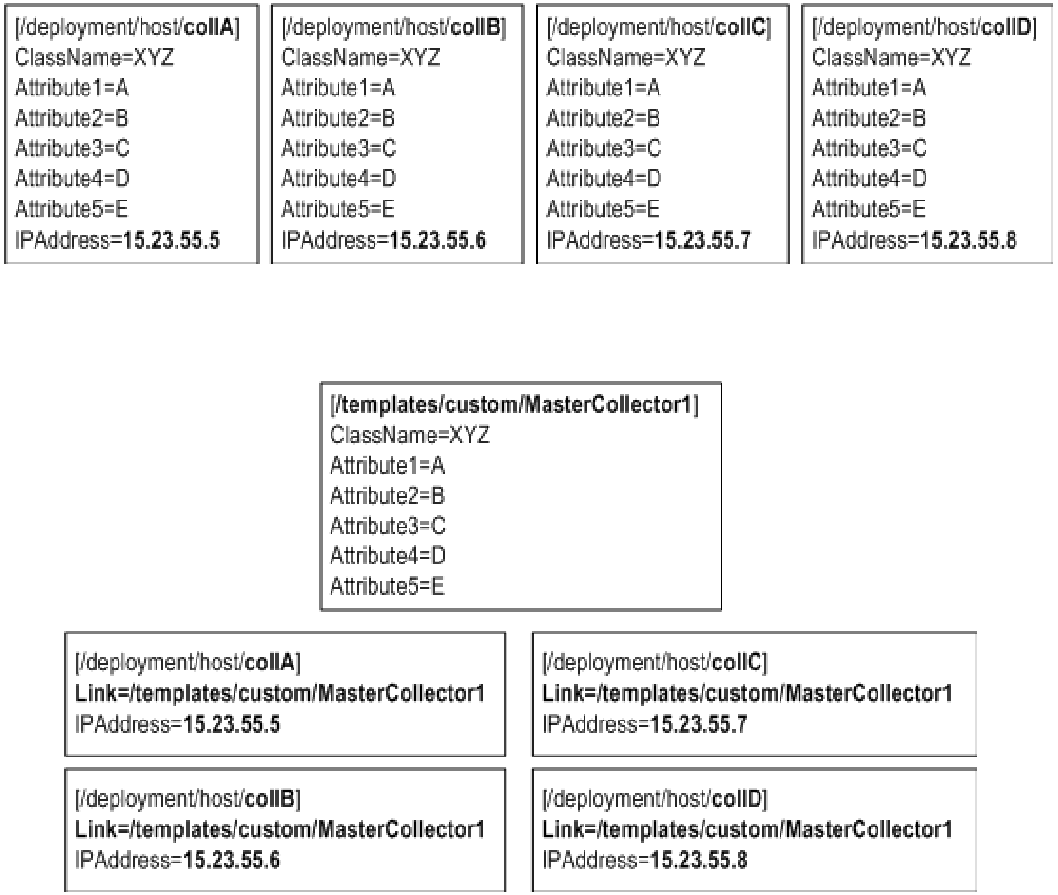
IUM Deployment – Creating Collectors

- Linked collectors are collectors that share a common configuration.
- Linked collectors greatly simplify the creation and management of multiple collectors that have nearly identical configurations.

Advantages of Linked Collectors

- Less configurations to manage. All the common configurations are kept in one place.
- Simple to change all linked collectors -- Just change the master and all collectors linked to the master are
- changed. Restart the collectors to make the change take effect.
- Faster creation of similar collectors.

IUM Deployment – Creating Collectors



```
[/deployment/host/collA]
ClassName=XYZ
Attribute1=A
Attribute2=B
Attribute3=C
Attribute4=D
Attribute5=E
IPAddress=15.23.55.5
```

```
[/deployment/host/collB]
ClassName=XYZ
Attribute1=A
Attribute2=B
Attribute3=C
Attribute4=D
Attribute5=E
IPAddress=15.23.55.6
```

```
[/deployment/host/collC]
ClassName=XYZ
Attribute1=A
Attribute2=B
Attribute3=C
Attribute4=D
Attribute5=E
IPAddress=15.23.55.7
```

```
[/deployment/host/collD]
ClassName=XYZ
Attribute1=A
Attribute2=B
Attribute3=C
Attribute4=D
Attribute5=E
IPAddress=15.23.55.8
```

```
[/templates/custom/MasterCollector1]
ClassName=XYZ
Attribute1=A
Attribute2=B
Attribute3=C
Attribute4=D
Attribute5=E
```

```
[/deployment/host/collA]
Link=/templates/custom/MasterCollector1
IPAddress=15.23.55.5
```

```
[/deployment/host/collC]
Link=/templates/custom/MasterCollector1
IPAddress=15.23.55.7
```

```
[/deployment/host/collB]
Link=/templates/custom/MasterCollector1
IPAddress=15.23.55.6
```

```
[/deployment/host/collD]
Link=/templates/custom/MasterCollector1
IPAddress=15.23.55.8
```

IUM Deployment – Testing Collectors

Whichever method you use to create a Collector,
you test them in the same way:

- In LaunchPad select the Collector
- Start the Collector in the Admin Tab
- Check the Collector **Status** in the Monitor Tab
- Check the Collector **Log file** in the Monitor Tab
- Check the Collector **Statistics** in the Monitor Tab
- **Clean-up** the Collector, if necessary, in the Monitor Tab

IUM Deployment – Testing Collectors

Typical Issues

- Referencing an Aggregation Scheme name that doesn’t exist
- Referencing an Aggregation Rule that doesn’t exist
- The No. of operations vs. elements don’t match
- Referencing an NME attribute that is not in the NME Schema
- Remember difference between NMEGroup vs. NME
  - NME is leaf node of aggregation tree
  - use NMEGroup at other levels
- No. of Parser fields doesn’t match no. of input fields
- Solid process or Admin Agent Process is not running
- Querying a session collector, but don’t use the “-session” flag - no data is returned

IUM Deployment – Testing Collectors

Typical Issues

- Loss of Network Connectivity or ConfigServer dies
  - If collector is up, it will continue to run
  - If trying to startup, will try to access, but then use locally saved config file
- No more space on file system
  - collector will stop; exceptions written to log
- IP Address for server changes
  - need to get new IUM License file
  - need to remove old CfgServer.ior file and restart the config server