Monitoring & SIEM & NOC/SOC

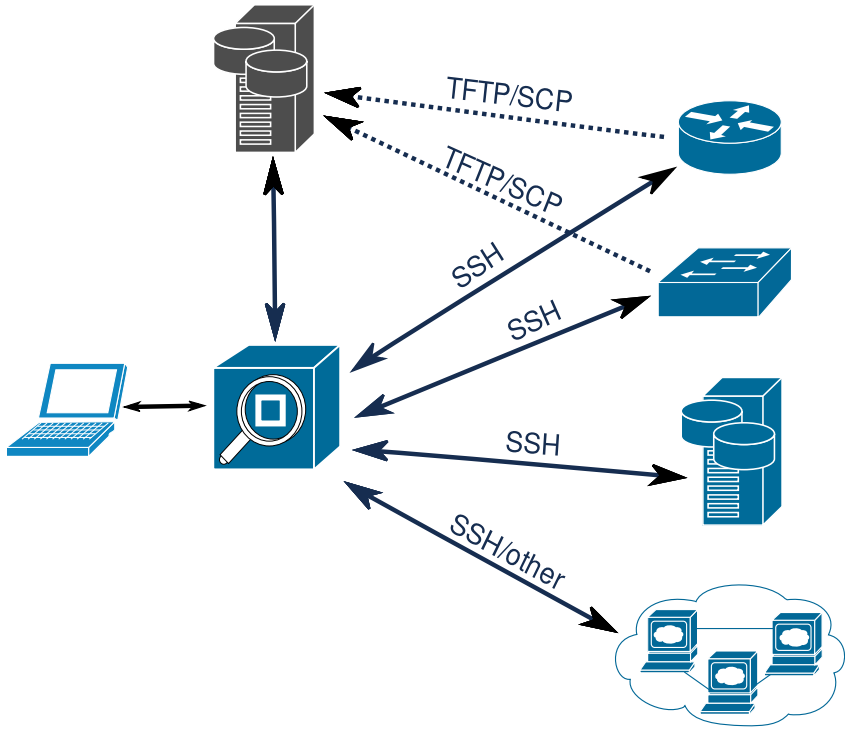
Segurança em Redes de Comunicações

Mestrado em Cibersegurança
Mestrado em Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

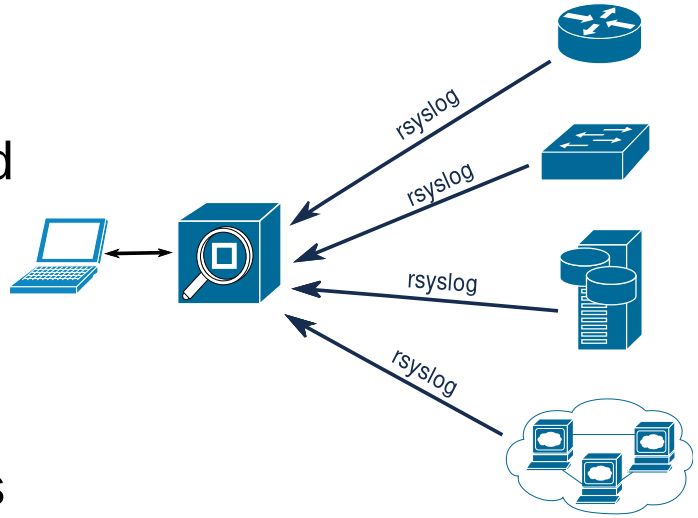
Remote CLI Access

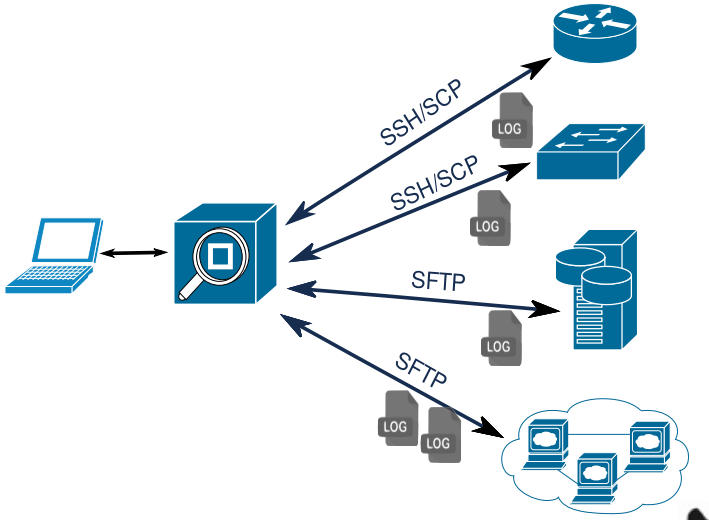
- Using a remote console to devices,
  - Using SSH, telnet (insecure), or proprietary protocols,
  - Retrieve configurations and device's processes status.
  - Devices can also upload configurations to a central point.
    - Using TFTP (insecure) or SFTP/SCP (many devices do not support it).
- Send “show” like CLI commands, retrieve output, parse information.



Log Files Access

- rsyslog
  - Able to accept inputs from a wide variety of services, transform them, and output the results to diverse network destinations.
    - Over TCP and/or SSL/TLS.
  - Timing controlled by monitored node/device.
  - Many post- and cross-processing tasks can be made on the monitored node/device.
- Direct access to log files
  - Using any remote access to remote files.
    - Requires special permissions.
  - SSH/SCP, SFTP, etc...
  - Timing controlled by central point.
  - Requires all heavy post- and cross-processing in a central point.



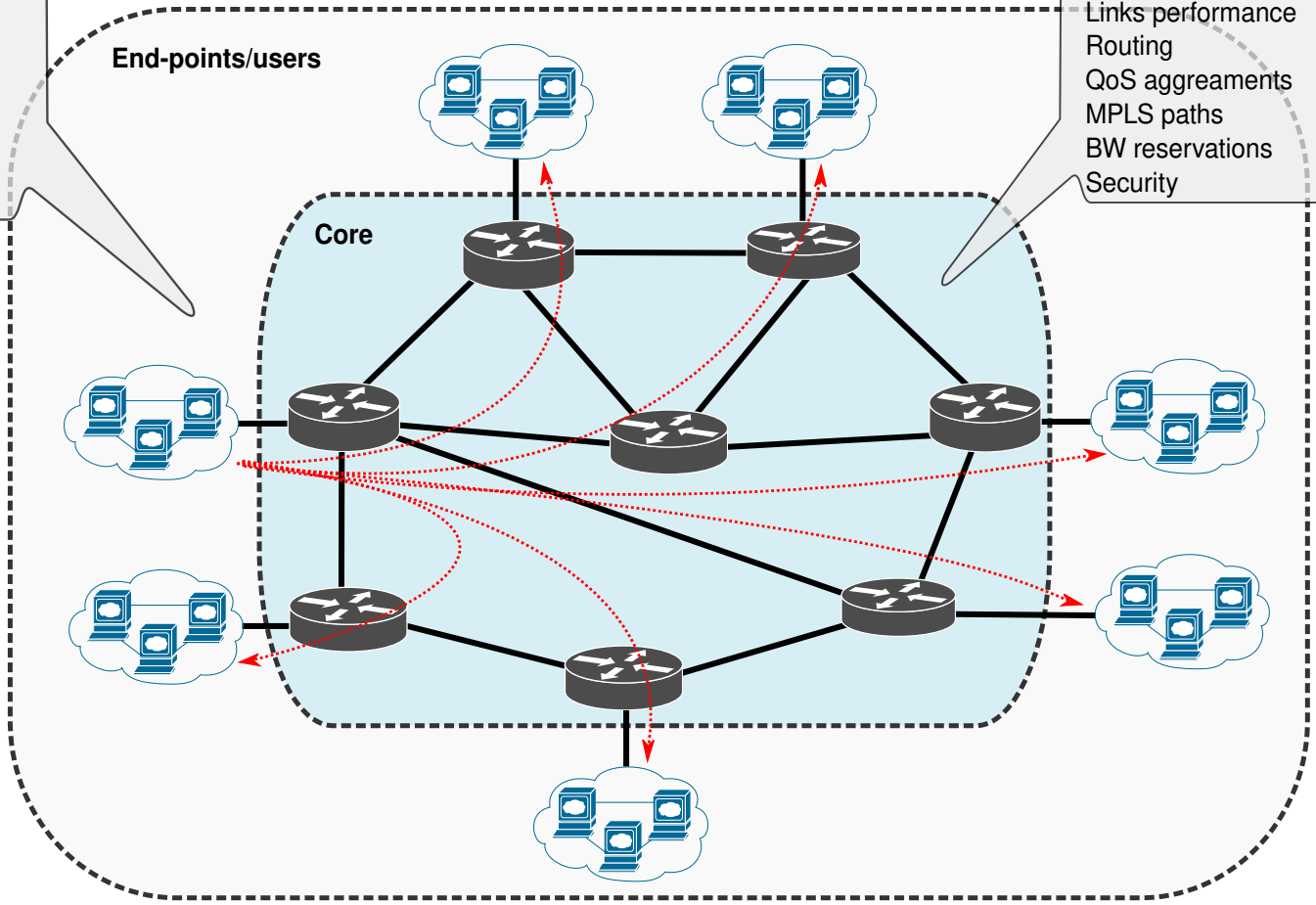


universidade de aveiro

Core and End-to-End Monitoring

End-to-end measurements
- delay
- jitter
- throughput
- losses
- BW reservations
- reserved paths validation

Demands per destination
- global
- per service/app
- per QoS usage



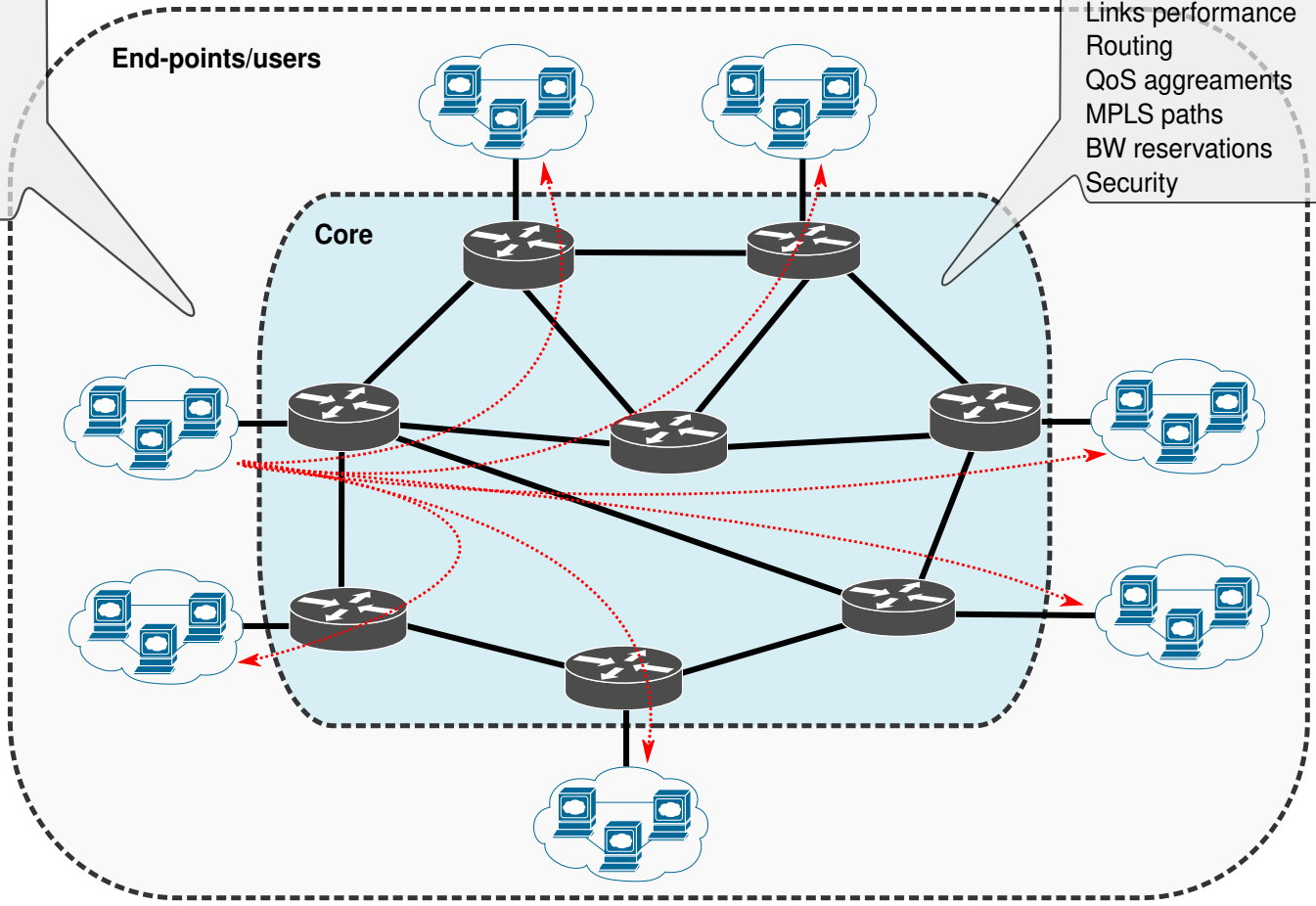
Core configurations
- Node awareness
- Service awareness

Nodes performance
Links performance
Routing
QoS aggreements
MPLS paths
BW reservations
Security

Core and End-to-End Monitoring

End-to-end measurements
- delay
- jitter
- throughput
- losses
- BW reservations
- reserved paths validation

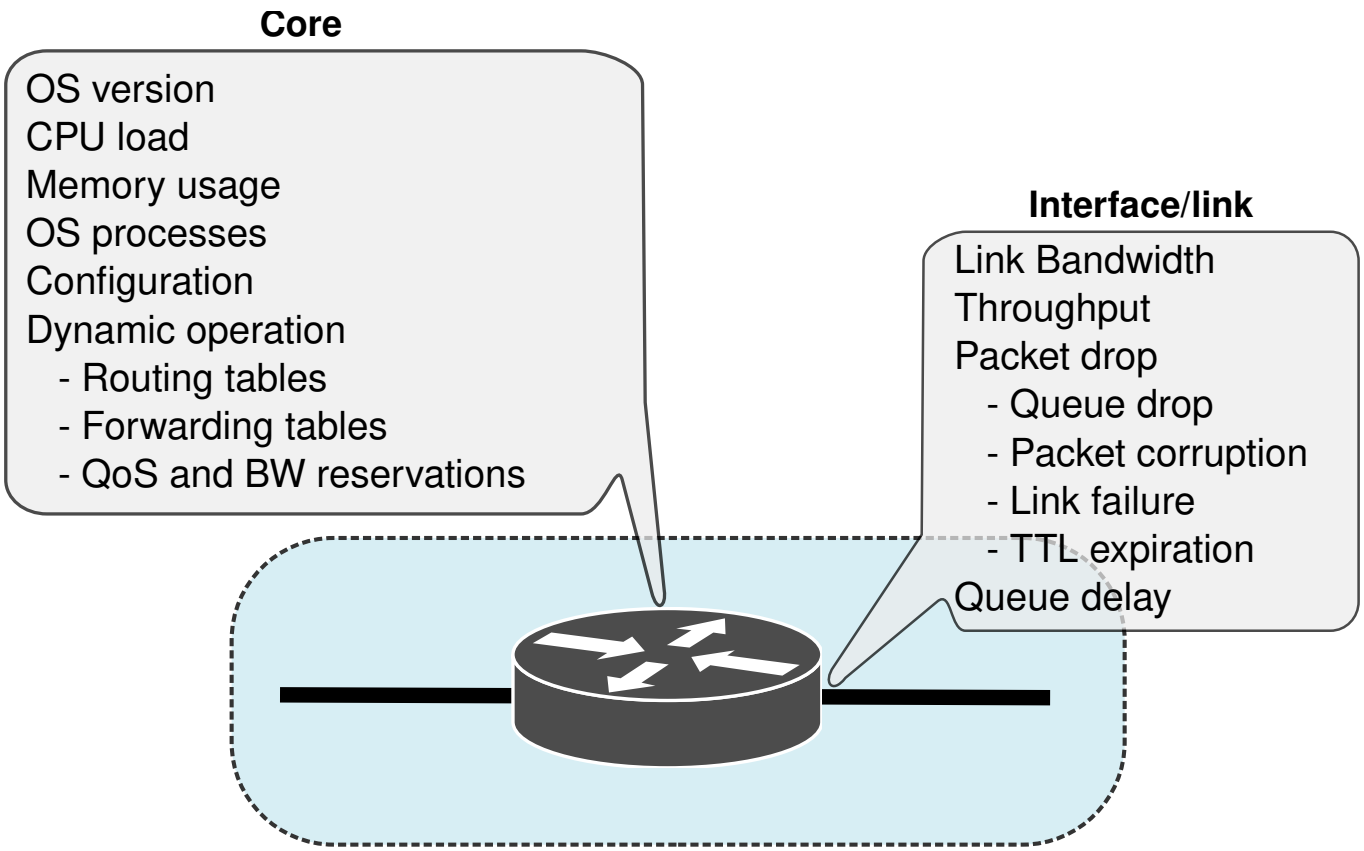
Demands per destination
- global
- per service/app
- per QoS usage



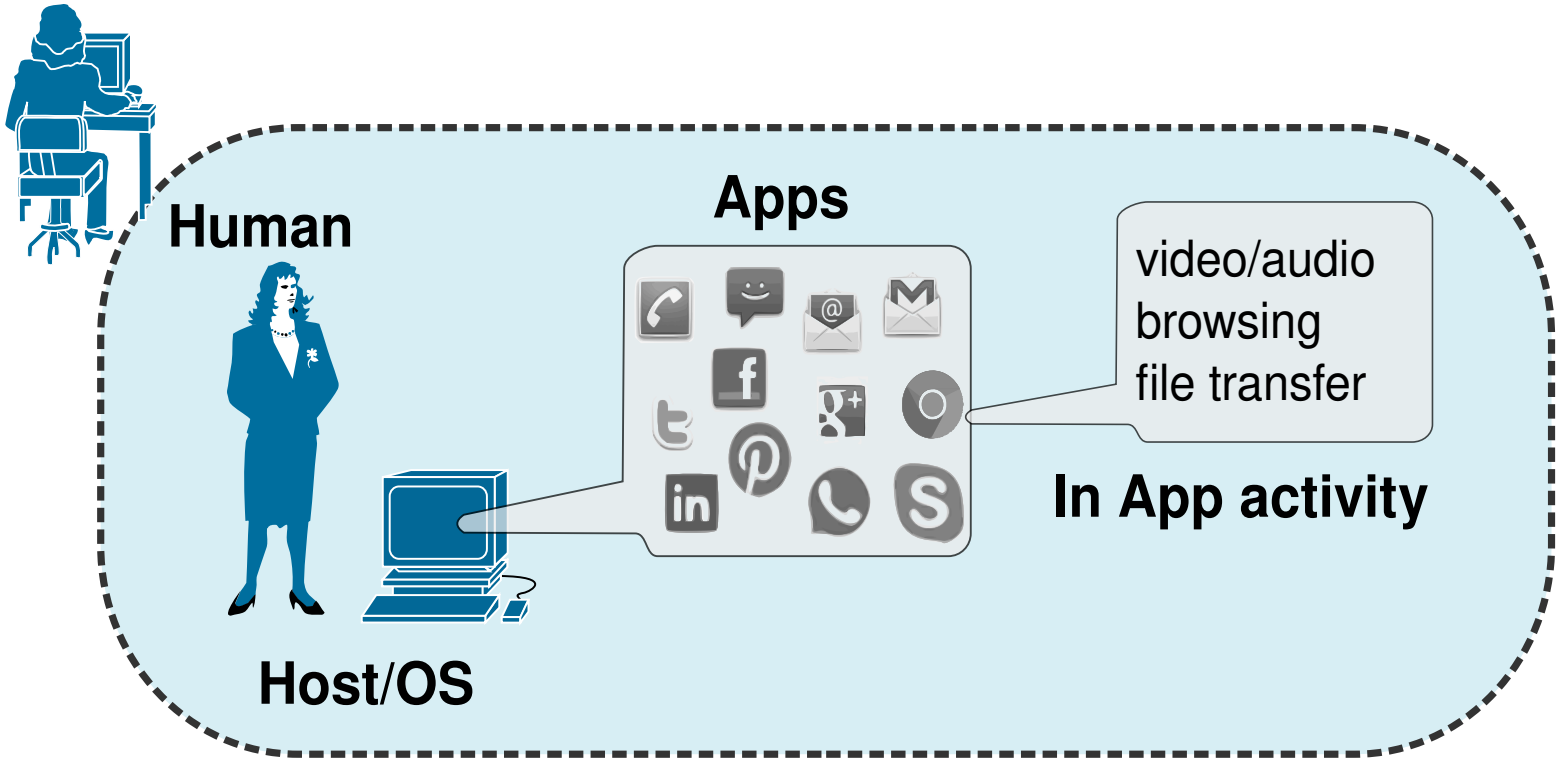
Core configurations
- Node awareness
- Service awareness

Nodes performance
Links performance
Routing
QoS aggreements
MPLS paths
BW reservations
Security

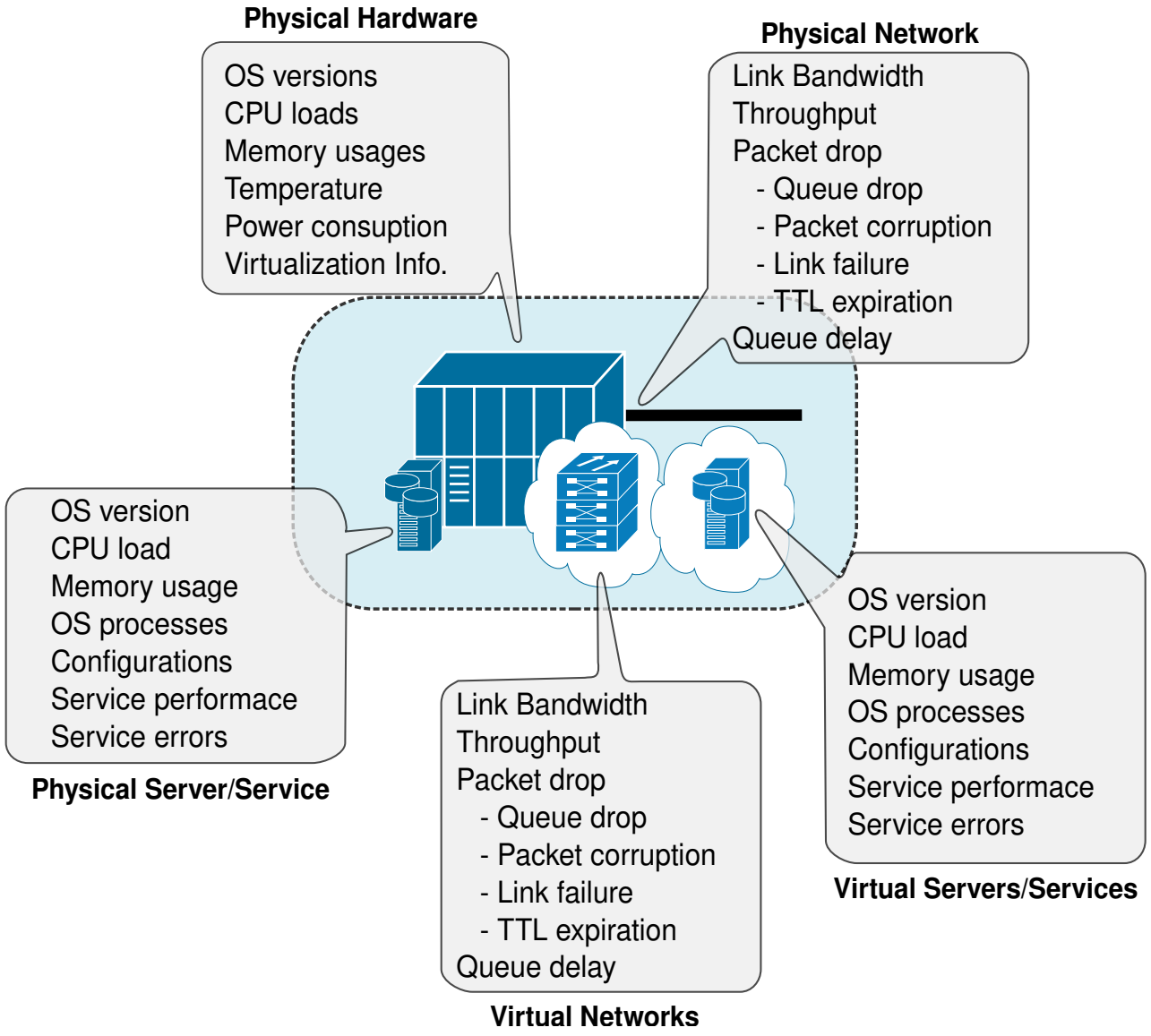
Node Monitoring



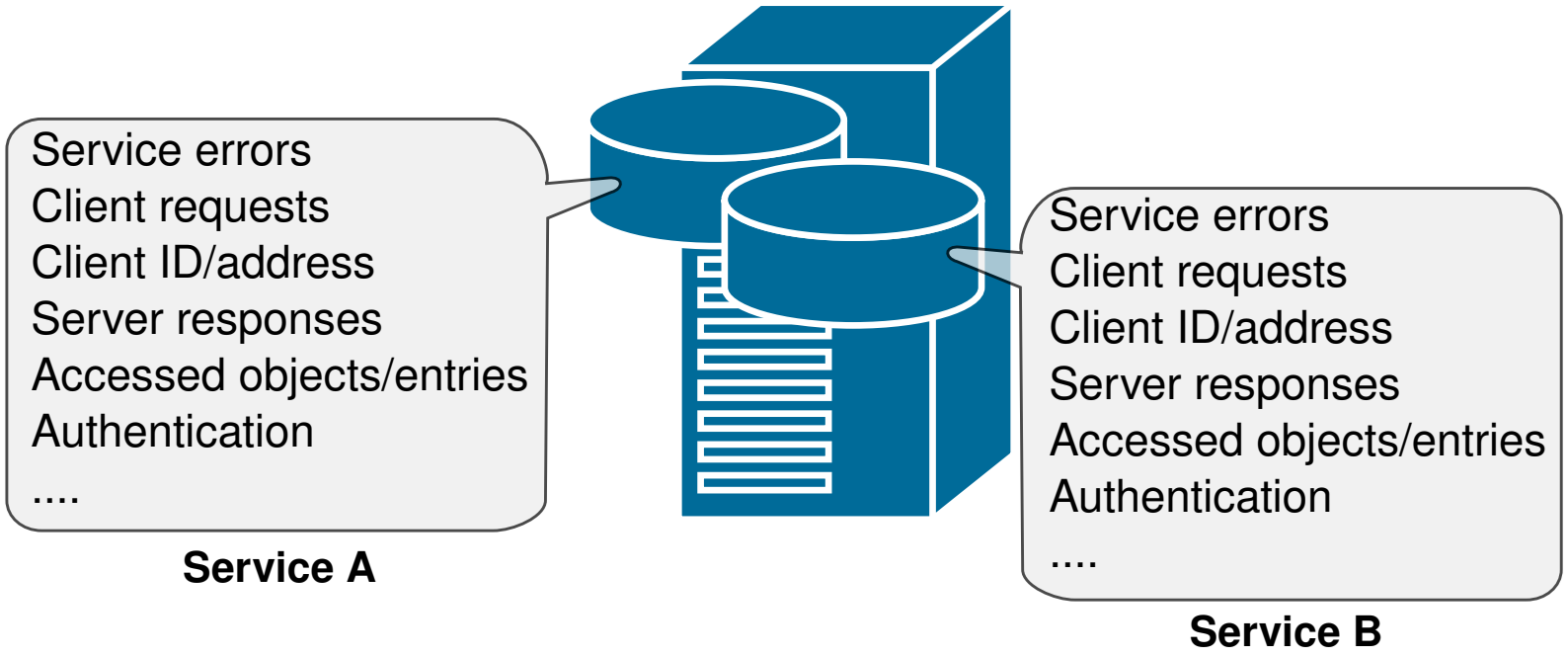
End-User/Host/App Monitoring



Server/Service/Cloud Monitoring



Per-Service Detailed Monitoring

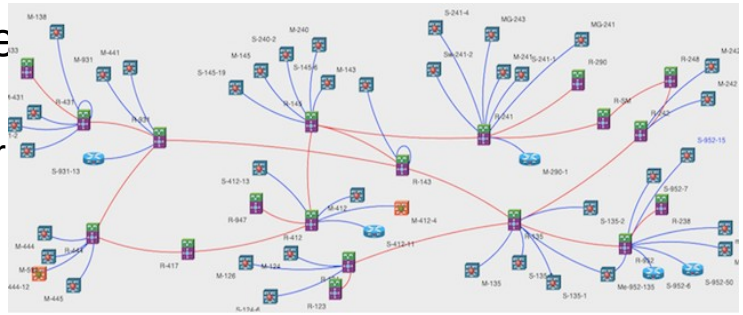


Data Sources

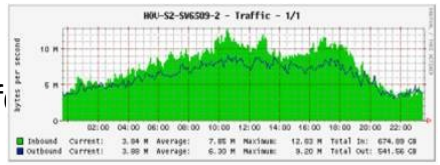
- SNMP
  - Used to acquire knowledge about current states of nodes/links/servers.
  - Local information. May be used to extrapolate to global information.
  - (Often) Requires the usage of vendor specific MIBs.
- Flow exporting
  - Used to characterize users/services in terms of amount of traffic and traffic destinations.
  - Medium and large time-scale information.
  - Protocols: Cisco NetFlow, IPFIX – Standard, Juniper jFlow, and sFlow
- Packet Captures / RAW statistics / DPI vs. SPI
  - Used to characterize users/services in small time-scales.
  - Requires distributed dedicated probes.
- Access Server/Device logs and/or CLI access.
  - Used to acquire knowledge about past and current state.
- Active measurements
  - Introduces entropy on network and requires (for many measurements) precise clock synchronization
  - E.g., one-way delay/jitter, round-trip delay/jitter.

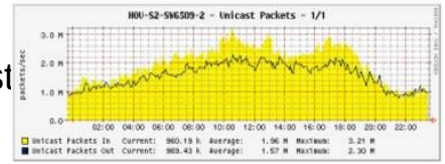
SNMP

- Used for acquiring the status and usage of node
  links and services over time.
  - Requires periodic pulling to obtain information over
- Used for obtain:
  - Network elements and interconnections,
  - Network deployed services.



- Used for estimating, characterizing, and predict:
  - Data flow performance.
    - Packet losses and (by indirect inference) delay/jitter at nodes.
    - Allows to obtain information about current and future service perf

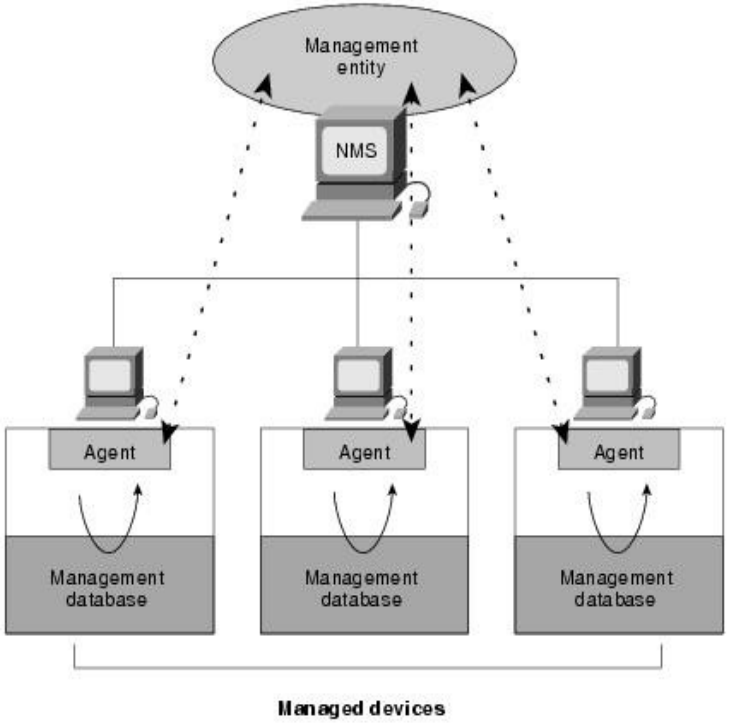




  - Nodes performance,
    - Memory/CPU usage, number of processes, etc...
    - Allows to detect points of failure, service degradation nodes, unst
  - Network link usage,
    - Ingress/egress bytes and packet counts.
    - Allows to perform optimizations in terms of routing (load balancing), link upgrade, and introduction of redundancy.
  - Data/flow routing,
    - At Layer 2, Layer 3 and MPLS levels.
    - Allows to understand how data flows and how may react to disruptive events.

SNMP Basic Components

- An SNMP-managed network consists of three key components:
- Managed devices
  - Network node that contains an SNMP agent.
  - Collect and store management information and make this information available using SNMP.
  - Can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
- Agents
  - Network-management software module that resides in a managed device.
- Network-management systems (NMSs)
  - Executes applications that monitor and control managed devices.
  - Provide the bulk of the processing and memory resources required for network management.
  - One or more NMSs must exist on any managed network.

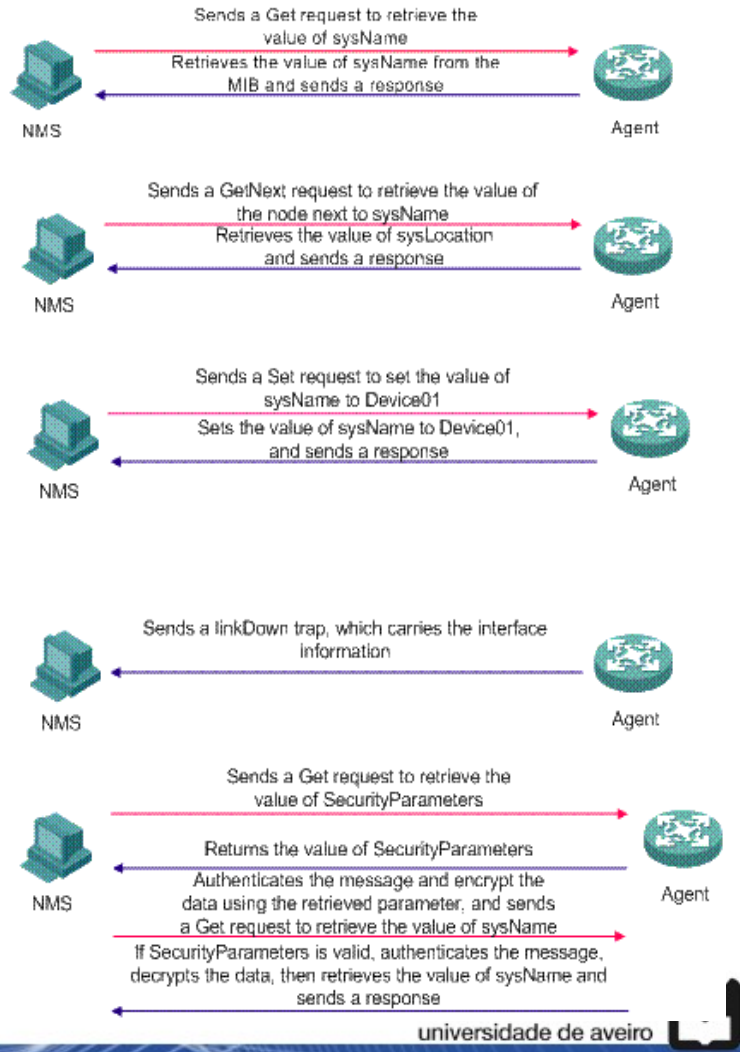


SNMP Versions

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

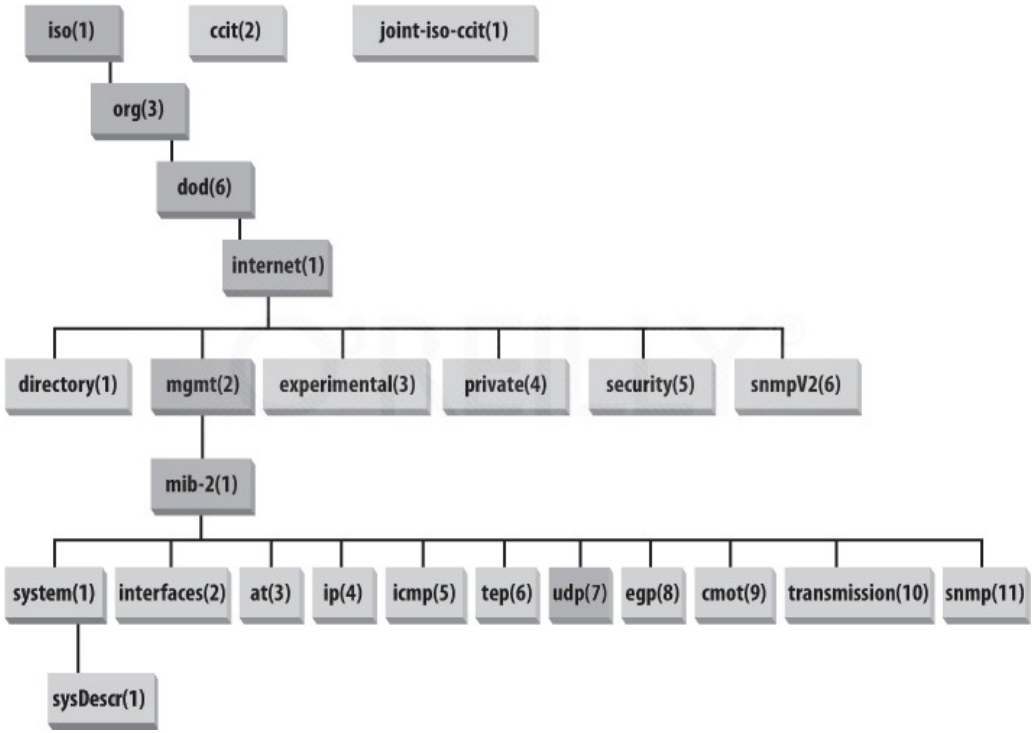
SNMP Operations

- SNMP provides the following five basic operations:
  - Get operation
    - Request sent by the NMS to the agent to retrieve one or more values from the agent.
  - GetNext operation
    - Request sent by the NMS to retrieve the value of the next OID in the tree.
  - Set operation
    - Request sent by the NMS to the agent to set one or more values of the agent.
  - Response operation
    - Response sent by the agent to the NMS.
  - Trap operation
    - Unsolicited response sent by the agent to notify the NMS of the events occurred.
- In SNMPv3 get operations are performed using authentication and encryption.



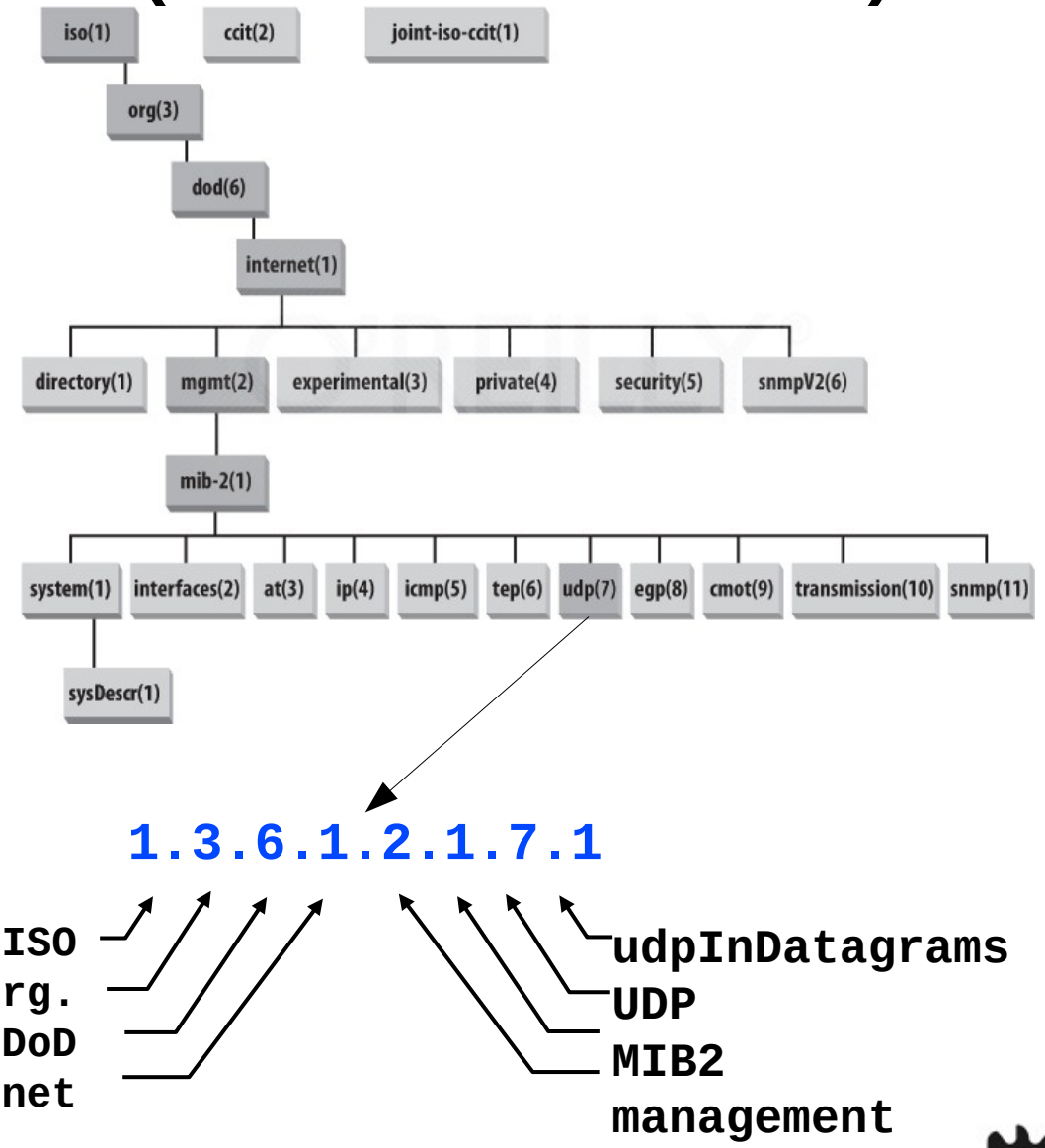
MIB Modules and Object Identifiers

- An SNMP MIB module is a specification of management information on a device
- The SMI represents the MIB database structure in a tree form with conceptual tables, where each managed resource is represented by an object
- Object Identifiers (OIDs) uniquely identify or name MIB variables in the tree
  - Ordered sequence of nonnegative integers written left to right, containing at least two elements
  - For easier human interaction, string-valued names also identify the OIDs
    - MIB-II (object ID 1.3.6.1.2.1)
    - Cisco private MIB (object ID 1.3.6.1.4.1.9)
- The MIB tree is extensible with new standard MIB modules or by experimental and private branches
  - Vendors can define their own private branches to include instances of their own products



SNMP Names (numbers/OID)

- To nominate all possible objects (protocols, data, etc.) it is used an ISO Object Identifier (OID) tree:
  - Hierarchic nomenclature of objects
  - Each leaf of the tree has a name and number



SNMP MIBs

- Management Information Base (MIB): set of managed objects, used to define information from equipments, and created by the manufacturer
- Example: UDP module

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Number of UDP datagrams delivered to users.
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Number of received UDP datagrams for which there was no application at the destination port.
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	The total number of UDP datagrams sent from this entity.

Relevant MIBs

- Interface characteristics, configurations, status, ans stats:
  - IF-MIB and IP-MIB.
  - Cisco extra information: CISCO-QUEUE-MIB, CISCO-IF-EXTENSION-MIB
- Nodes management information (description, general information, CPU/memory status, etc...):
  - SNMPv2-SMI and ENTITY-MIB.
  - Vendor specific: CISCO-SMI, JUNIPER-SMI, etc...
  - Cisco extra: CISCO-PROCESS-MIB, CISCO-FLASH-MIB, CISCO-ENVMON-MIB, CISCO-IMAGE-MIB, etc...
- Node routing and traffic-engineering:
  - IP-MIB, IP-FORWARD-MIB
    - Cisco extra information: CISCO-CEF-MIB, CISCO-PIM-MIB
  - MPLS-TE-MIB, MPLS-LSR-MIB, MPLS-VPN-MIB
- Node services:
  - Vendor specific: CISCO-AAA-SESSION-MIB, CISCO-SIP-UA-MIB, etc...
- Node monitoring mechanisms:
  - RMON-MIB, RMON2-MIB, CISCO-SYSLOG-MIB, CISCO-RTTMON-MIB, CISCO-NETFLOW-MIB, CISCO-IPSEC-FLOW-MONITOR-MIB, etc...

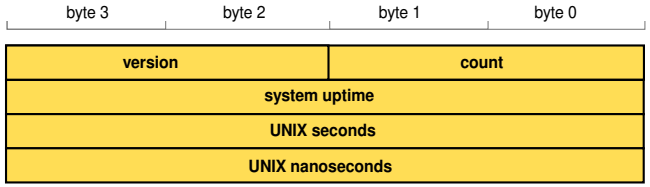
NetFlow

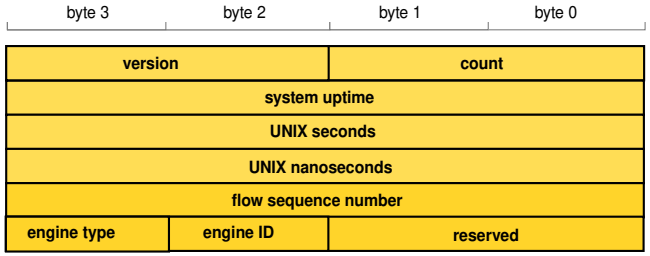
- Cisco NetFlow services provide network administrators IP flow information from their data networks.
  - Network elements (routers and switches) gather flow data and export it to collectors.
  - Captures data from ingress (incoming) and/or egress (outgoing) packets.
  - Collects statistics for IP-to-IP and IP-to-MPLS packets.
- A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device.
  - A flow is identified as the combination of the following key fields:
    - Source IP address, Destination IP address, Source port number, Destination port number, Layer 3 protocol type, Type of service (ToS), and Input logical interface.
- These collected flows are exported to an external device, the NetFlow collector.
- Network flows are highly granular
  - For example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, autonomous system numbers, etc.
- NetFlow has three major versions: v1, v5 and v9.
  - v1 is only recommended for legacy devices without support to v5 or v9.
  - V1 and v5, do not support IPv6 flows.

NetFlow versions 1 and 5

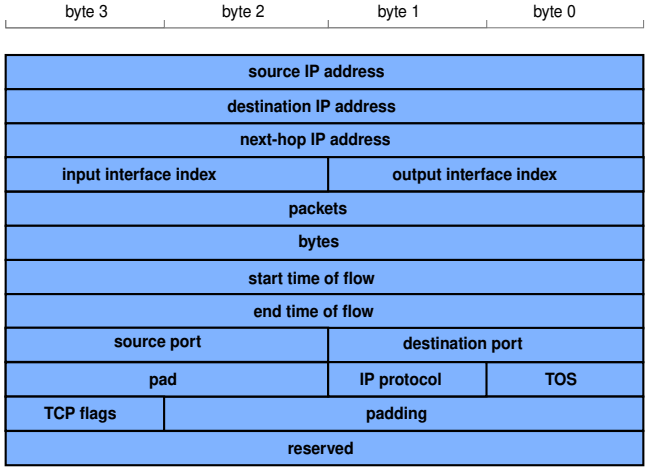
- NetFlow v1/v5 packets are UDP/IP packets with a NetFlow header and one or more NetFlow data Records

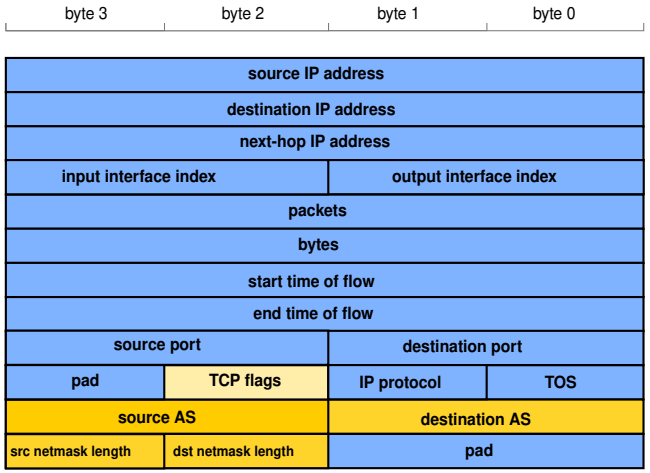
Header format





Record format



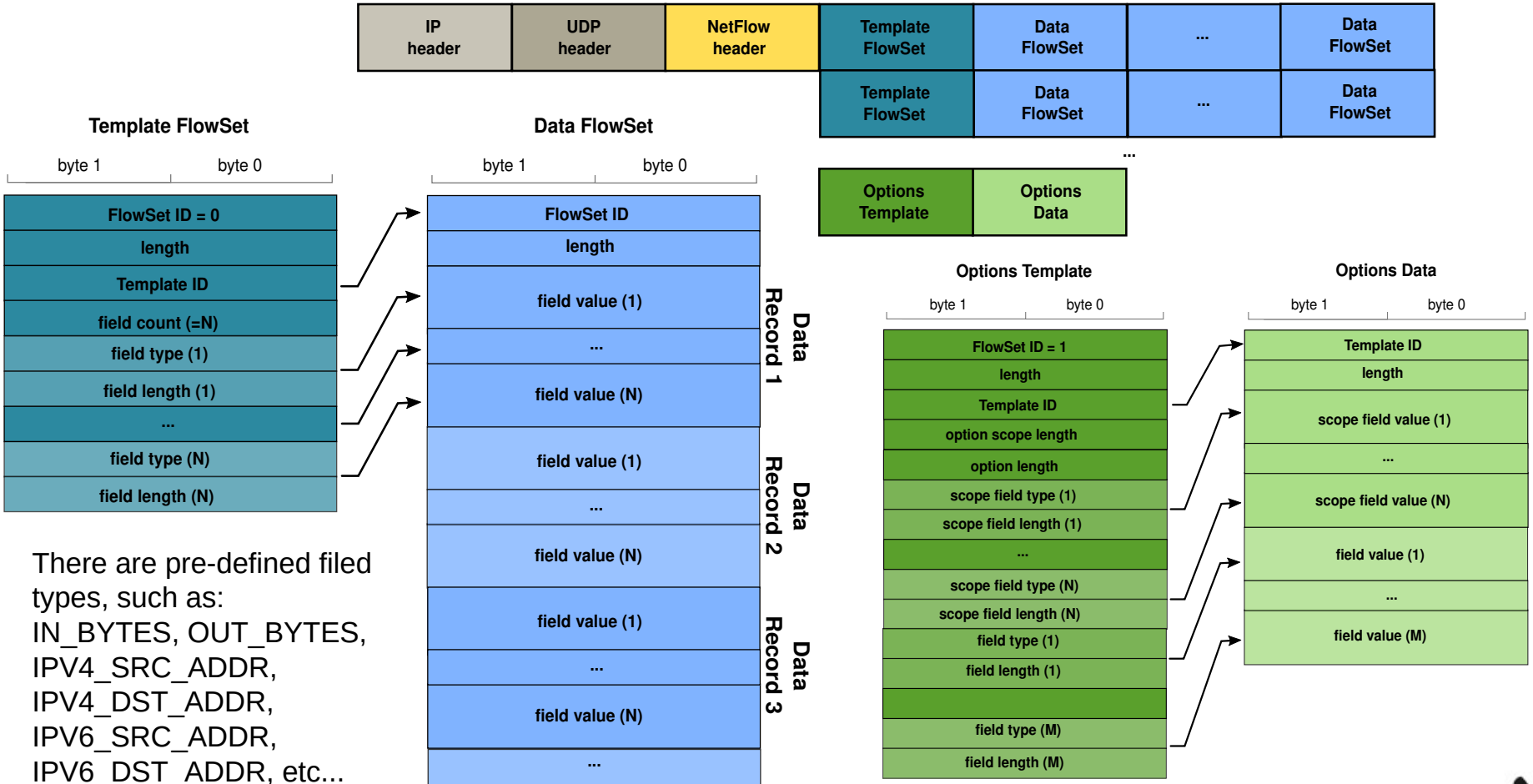


Version 1

Version 5

NetFlow version 9

- NetFlow v9 packets are UDP/IP packets with a NetFlow header, one or more Template FlowSets (may be suppressed, if sent previously), one or more Data FlowSets, and, optionally, an Options Template and Data Record.



There are pre-defined filed types, such as:
IN_BYTES, OUT_BYTES,
IPV4_SRC_ADDR,
IPV4_DST_ADDR,
IPV6_SRC_ADDR,
IPV6_DST_ADDR, etc...

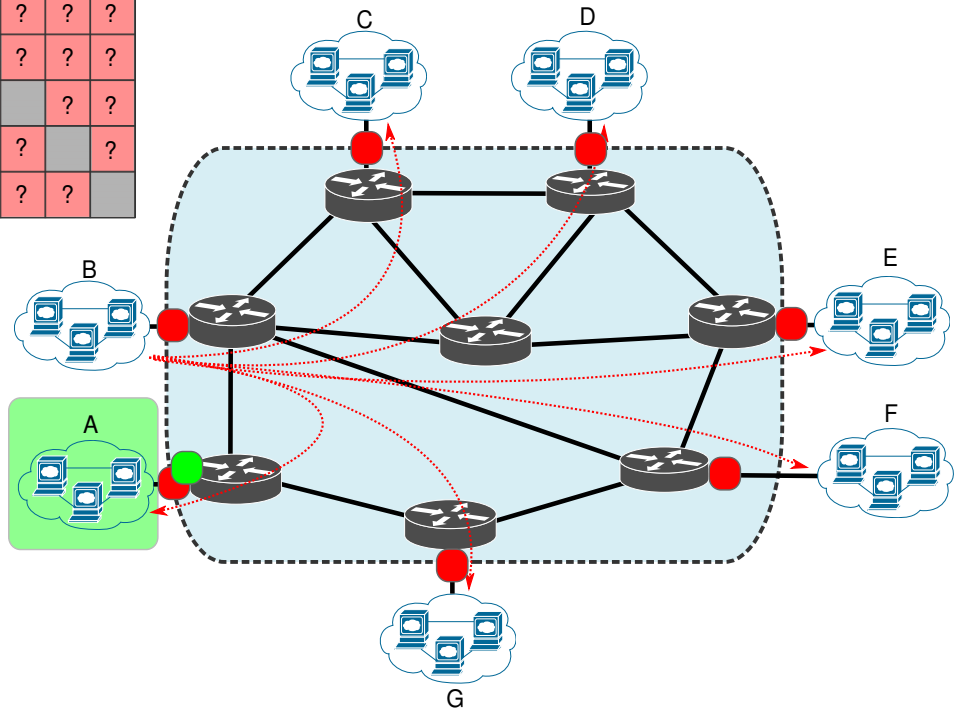
NetFlow Usage

- Used to characterize users/services in terms of amount of traffic.
  - Users/Groups (overall or per-app) → Applied in (V)LAN interfaces.
  - Services → Applied to data-center interfaces
- Used to characterize traffic destinations (to egress points) from a specific ingress point in a network: traffic matrices.
  - Ingress/Egress points may be:
    - Network access links (distribution layer L3SW, Internet access routers, user VPN server links),
    - Network core border links (core border routers),
    - BGP peering links (AS Border routers).
- Used to characterize “in network” routing.
  - Complex to implement and process.

NetFlow Deployment

- Interfaces to monitor depend on objective:
  - Traffic matrix inference – all core border interfaces.
  - User/group flow generation inference - access interface from user/group.
- Egress vs. Ingress monitoring:
  - Traffic matrix inference – ingress OR egress.
  - User/group flow generation inference – both directions.

	A	B	C	D	E	F	G
A		?	?	?	?	?	?
B	?		?	?	?	?	?
C	?	?		?	?	?	?
D	?	?	?		?	?	?
E	?	?	?	?		?	?
F	?	?	?	?	?		?
G	?	?	?	?	?	?	

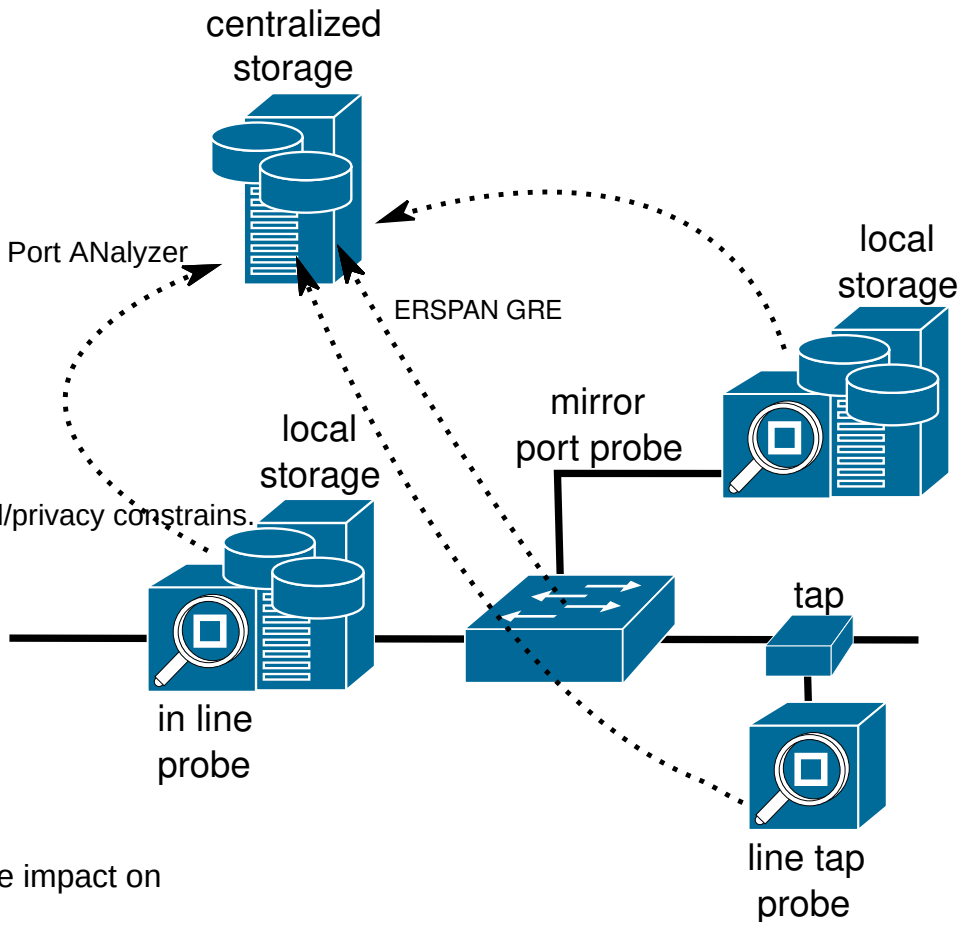


IPFIX (v10) and Flexible NetFlow

- IPFIX is very similar to NetFlow v9
  - Uses version 10 in a similar header.
  - Also has Templates and Data Records.
  - Also has Options Templates and Options Data Records.
- IPFIX made provisions for NetFlow v9 and added support for it.
  - IPFIX lists an overview of the “Information Element identifiers” that are compatible with the “field types” used by NetFlow v9.
- IPFIX has more filed types than the ones defined for NetFlow v9.
  - Also allows a vendor ID to be specified which a vendor can use to export proprietary/generic information.
- IPFIX allows for variable length fields.
  - Useful to export variable size strings (e.g., URLs).
- NetFlow v9 extension “Flexible NetFlow” aims to be equally flexible as IPFIX.

Network Passive Probing

- User for:
  - Specific and detailed data inference,
  - Infer small and medium timescale dynamics.
- Probe types
  - Switch mirror port,
  - In-line,
  - Network tap.
  - ERSPAN GRE tunnel from switch.
    - ERSPAN: Encapsulated Remote Switched Port ANalyzer
- Filtering/sampled by
  - User/terminal address/VLAN/access port,
  - Group address/VLAN/access port,
  - Protocols (UDP/TCP),
  - Upper layer protocols,
    - Hard to identify due to encryption and legal/privacy constrains.
  - UDP/TCP port number/range.
- Data processing
  - Packet/byte count,
  - Flow count,
  - IP addresses and port distribution,
  - App/service statistics and distribution.
- Local vs. Centralized storage and processing.
  - Data upload to centralized point should not have impact on measurements.
  - Local storage/processing requires probes with more resources.



Log Management Systems (LMS)

- Software system that aggregates and stores log files from multiple network sources and systems.
- Allows organizations to centralize all of their log data from multiple systems.
- Allows Logs to be viewed and correlated.
- Main purposes:
  - Detect and respond to Indicators of Compromise (IoC);
  - Conduct forensic data analysis;
  - Perform investigations into network events and possible attacks.

Security Information and Events Management (SIEM)

- Incorporates three types of security tools into a single application:
  - Security Event Management (SEM)
    - Very similar to LMS.
    - Aggregates log files from multiple systems, but they are more geared towards the needs of IT security analysts instead of system administrators.
  - Security Information Management (SIM)
    - Software tools used to identify, collect, and analyze data from event logs.
    - Include automated features and alerts that can be triggered when predetermined conditions are satisfied that might indicate that the network is compromised.
    - Help security analysts automate the incident response process and generate more precise reports on the organization's security position/past.
  - Security Event Correlation (SEC)
    - Software used to process ans search massive quantities of event logs and discover correlations and connections between events that could indicate a security issue.

LMS vs. SIEM

- LMS tools are more focused on:
  - Log Data Collection, efficient Retention of Data, log indexing and search functions, ans reporting.
- SIEM tools are more focused on:
  - Threat detection alerts, event correlation, and dash-boarding (real-time monitoring with custom events visibility).
- Evolution of traditional LMS, designed mainly for system administration support, made them functionally much closer to SIEM tools developed from scratch as a security tool.

SIEM Events (examples)

- Brute force detection
  - Excessive 404 errors (HTTP server Log) from a non-authenticated client (DB Log).
  - Excessive login failures (services or DB Logs) at one or multiple services.
    - From a specific IP address (or set of IP addresses).
    - From “strange” geographic regions or AS.
  - Non-matching credentials
    - From internal machines with non-matching user credentials (RADIUS/LDAP Logs).
- Impossible travel
  - Multiple logins from same user from different devices/locations.
  - Consecutive logins from same user from distant geographic regions within a small time window. VPN usage may trigger such an alarm.
- Anomalous data transference
  - Analyzing by individual source (IP or device group) and/or destination and/or by used protocol/port.
  - Excessive/Different data transference not compatible with past observations
    - Protocols and ports usage;
      - Usually firewall rules solve this!
    - Download/upload amounts, number of connections, ratio upload/download, ratio DNS/non-DNS, etc…;
    - Never contacted devices: external servers (unknown IP/ASN or country) or internal devices,;
    - Absolute time of day/week/month.
    - Relative time activity: mean or standard deviation of intervals between activity/flows/requests/etc...
  - Should be used to detect exfiltration (or propagation inside the network) and illicit C&C and data channels.
- DDoS attack
  - Excessive connection attempts from “never seen” devices/addresses/regions.
    - Ideal detection in the early phase of the attack.
  - Non-excessive attempts, but non-conformal behavior (time behavior, sequence of requests,etc...)
    - More difficult to define.
- Files/Configurations integrity fails
  - Specific device/service configuration file checksum failure, non justifiable by observed actions.
  - Generic file checksum failure, non justifiable by observed actions.
- Etc… ?

Security Operations Center (SOC)

- Competences of a SOC in an organization:
  - Prevention and detection of attacks
    - Monitor network and services (with SIEM)
    - Detect vulnerabilities (with vulnerability scanning tools)
    - Detect malicious activities (with SIEM)
    - Detect anomalous behaviors (with SIEM)
      - may not be malicious!
  - Investigation
    - Analyze the suspicious activity to determine/characterize the threat
    - Evaluate how deep the threat has penetrated the network/systems
  - Response
    - Deploy counter measures based on known playbooks
    - Deploy emergency measures when threat do not match a known response playbook
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response
- Nowadays commonly operated independently of the Network Operation Center (NOC).
- Should be integrated with NOC.
  - For network/services segregation and resilience, data acquisition and threat mitigation.

Security Metrics/KPI

- Access management
  - How many users have administrative access, and how often is used.
  - Shared passwords between staff.
- Preparedness
  - Percentage of devices fully patched and up to date.
- Days to patch
  - Average time between patch availability and deployment.
- Unidentified devices
  - Illicitly deployed devices.
  - BYoD policy, legacy devices, unlisted devices, IoT devices, etc...
- Security devices average/maximum load per time period.
- Intrusion attempts
  - Amount of detected and undetected attempts (in real time or after off-line auditing).
- Cost per incident
  - Includes staff overtime, external support, investigation costs, employee productivity loss, loss of communication, service failure, etc…
- Mean Time Between Failures (MTBF)
  - Average time between failures (hardware and/or software).
  - General or per device/service.
- Mean Time to Recovery (MTTR)
  - Average time between failure and recovery (hardware and/or software).
- Mean Time to Detect (MTTD)
  - Average time between intrusion and detection.
- Mean Time to Acknowledge (MTTA)
  - Average time between detection and start of countermeasures deployment.
- Mean Time to Contain (MTTC)
  - Average time between start of countermeasures deployment and complete mitigation.
- Mean Time to Resolve (MTTR)
  - MTTA+MTTR