Cyber Situational Awareness

Técnicas de Perceção de Redes

Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro

deti.ua.pt

Awareness

- **Direct** Awareness
  - By direct observation.
- **Indirect** Awareness
  - By analysis of reactions to events.
- Awareness **by Correlation**
  - Joint analysis of multiple sources of data to detect hidden patterns and relations.
  - Big Data Problem.
- Awareness **by Prediction**
  - Detection of patterns over time.
  - Black Swan Problem!
- Its all an **Inference**, **Validation**, **Correction** loop.

Cyber Situational Awareness (1)

- Ability to effectively **Acquire Data** by **Monitoring** networks and systems to:
  - Optimize services,
  - Detect and counter-act anomalous activity/events.
- **Analyze/Process** data to know and characterize
  - Network entities,
    - An entity should be understood as a person, a group, a terminal, a server, an application, etc...
  - Data flows,
  - Services and users perception of service.

Cyber Situational Awareness (1)

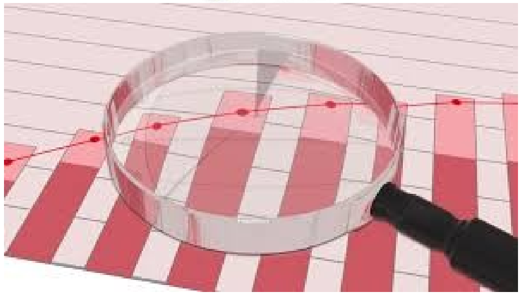
- All data sources are acceptable.
  - Never assume data irrelevance!
- Data may be:
  - Quantitative.
    - Allows for statistical analysis and may serve as machine learning training input.
    - e.g., number of packets, number of flows, number of contacted machines, etc...
  - Qualitative.
    - Can be transformed to quantitative data by counting techniques and statistical characterization
    - e.g., error message X, address Y contacted, packet of type Z, etc...

Cyber Situational Awareness (1)

- Time is relevant.
  - Relative and absolute.
  - An event occurs in a specific time instant, and it is part of a sequence of events.
- Timescale(s) of analysis must:
  - Include the target characteristics,
  - Allow the perception of the event in time for a response.
- Data may be re-scaled for multiple analysis purposes.

Situational Awareness Steps

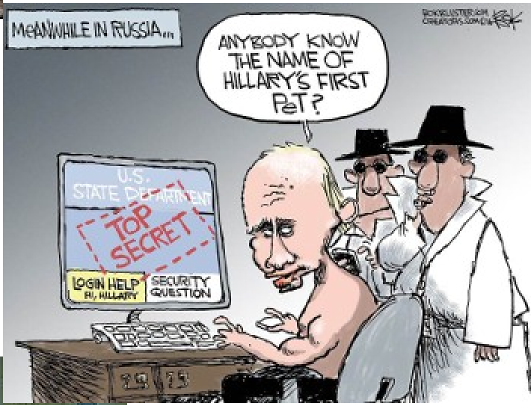
- Data acquisition.
- Data processing.
    - Creation of time sequences with different counting intervals (minimum timescales).
    - Creation of time sequences with different statistical metrics (larger timescales).
- Creation of entities' behavior profiles.
    - Usually time dependent.
- Classification of entities' behaviors.
    - Identification/classification.
    - Anomaly detection.



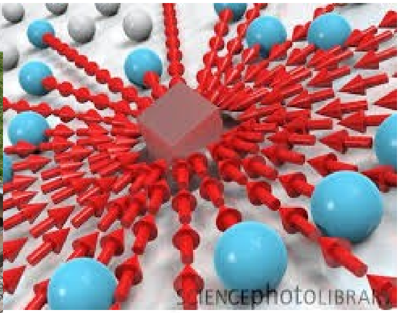
Network Atack Vectors

Type of Attacks (1)

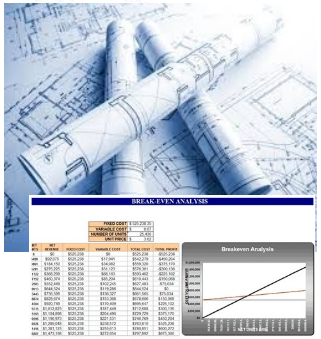
- Objectives:
  - Fun and/or hacking reputation
  - Political purposes
  - Military purposes
  - Economical purposes
  - Other?
- Technical objectives:
  - Operation disruption
  - For data interception
  - Both
    - Disruption to intercept!
    - Intercept to disrupt!



Type of Attacks (2)

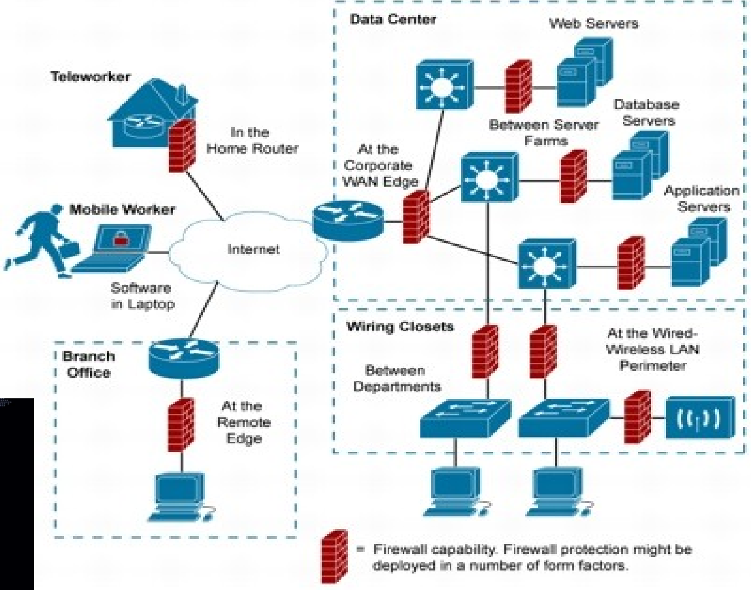


- Technical objectives:
  - Operation disruption.
    - (Distributed) Denial-of-Service.
  - Resources hijack.
    - Spam,
    - Crypt-currency mining/masternodes,
    - Platform to other attacks!
  - Data interception/stealing.
    - Personal data
      - As final goal,
      - Or as tool to achieve more value information!
    - Technical data,
      - Usually used to achieve more value information!
    - Commercial data
      - Digital objects, financial and/or engineering plans, ...
- Disruption may be used to achieve interception!
- Interception may me used to achieve disruption (operational or commercial)!



Traditional Defenses

- Vulnerability patching.
- Firewalls
  - Centralized.
  - Distributed.
- Intrusion Prevention and Detection Systems (IDS/IPS).
- Antivirus.

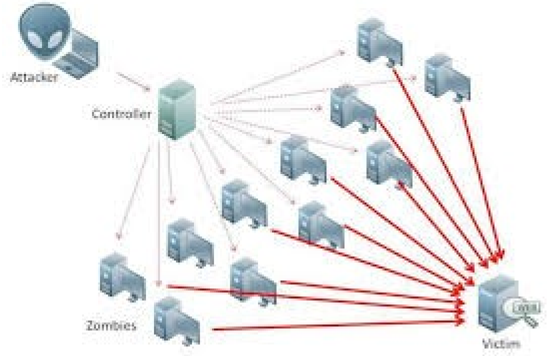


- **All rely on previous knowledge of the threat and/or problem!**

“Intelligent” Defenses

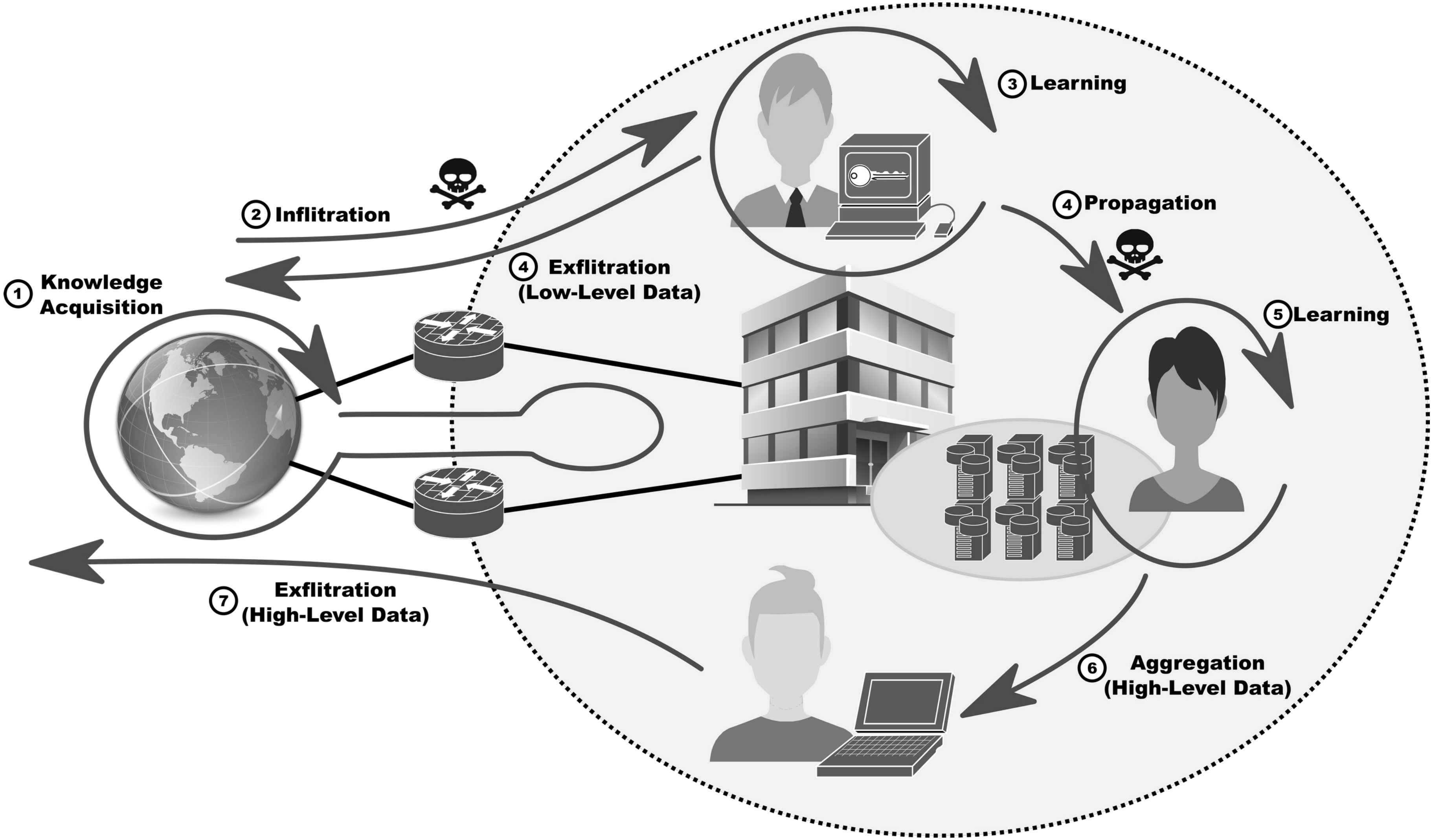
- Detection of unknown threats and/or problems.
  - In time to deploy counter-measures.
- Application of Big Data and Data Science techniques to network ans systems monitoring data.
- Some traditional solutions start to incorporate AI into their equipment
  - E.g., Palo Alto Network Firewalls, Cisco Appliances, …
- Still limited to manufacturer based solutions and localized data.
- Still limited in scope.
  - Obvious threats vs. Stealth threats.
- Optimal deployment requires an overall network and systems knowledge.
  - Network and Systems (Cyber) Situational Awareness.

Disruption Attacks



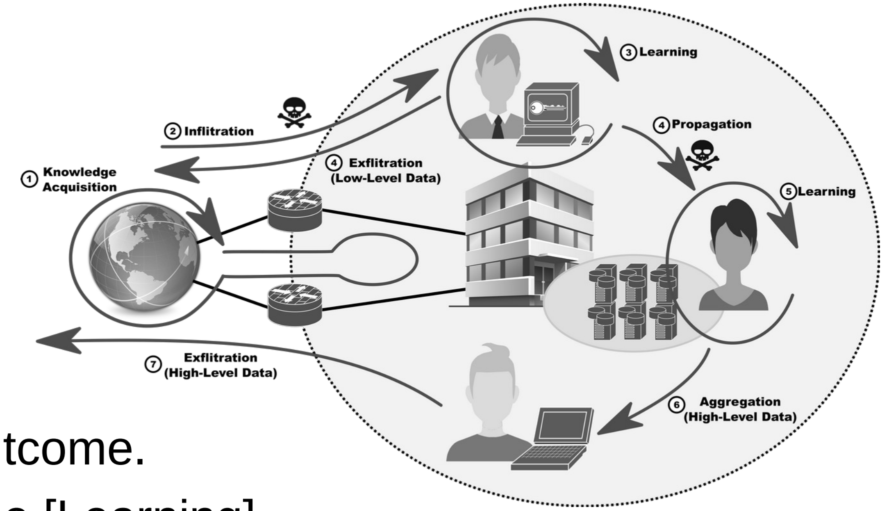
- Distributed DoS
  - Multiple slow/small devices generating traffic to a target
    - TCP vs. UDP
  - Purpose of disruption
    - By political/economical/"reputation"
    - Redirection to other service/location?
  - Solution at target
    - Load-balancers
    - For TCP, maybe its possible to survive making active (with licit client validation) session resets (server/firewalls)
      - White list solution, for completed session negotiation
    - For UDP/DNS, block requests for known external relay/redirection DNS servers (blocks attack amplification, IP target spoofing)
      - Doesn't work with large botnets and direct requests to target
  - Solution at source
    - Anomalous behaviors detection
      - Low traffic variations hard to detect
      - Time and periodicity changes are easier to detect
      - Destinations of traffic changes
      - With "really low" data rates is impossible to detect
- Denial o service by physical signal jamming
  - Pure disruption, or
  - Disruption to activate secondary channels (more easily compromised).
  - Solution
    - Detect, localized source and physically neutralize.

More Advanced Attacks Phases



1 Knowledge Acquisition
2 Infiltration
3 Learning
4 Propagation
4 Exfiltration (Low-Level Data)
5 Learning
6 Aggregation (High-Level Data)
7 Exfiltration (High-Level Data)

Attacks are Done Incrementally



① Knowledge Acquisition
② Infiltration
③ Learning
④ Propagation
④ Exflitration (Low-Level Data)
⑤ Learning
⑥ Aggregation (High-Level Data)
⑦ Exflitration (High-Level Data)

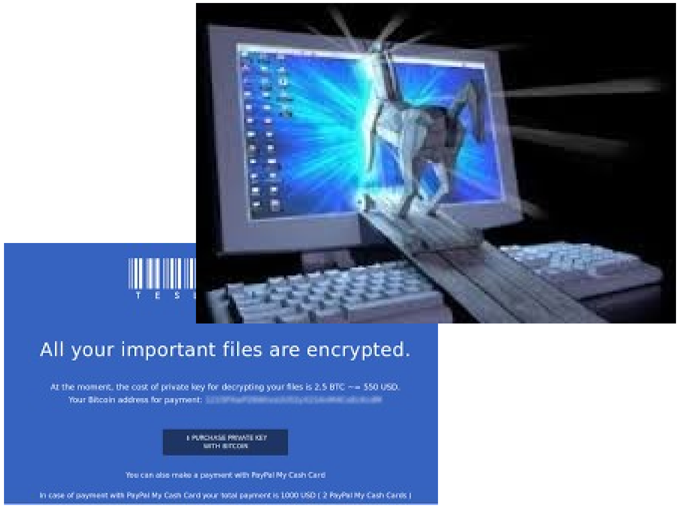
- Escalation of goals and privileges.
  - Public knowledge opens doors to private information and access to protected domains [Infiltration].
  - The first illicit access to a protect domain may not provide a relevant outcome.
  - Attacker must acquire more knowledge [Learning].
  - The additional knowledge allows to access other secure domain zones/devices/data with increasing relevance [Propagation].
    - At any phase the attacker may require additional knowledge [Learning].
  - When a relevant outcome is acquired it must be transfered to outside of the protected domain [Exfiltration].
  - Direct exfiltration may denounce the relevant points inside of the secure domain.
    - The relevant outcome must be first transferred inside the protected domain to a less important point [Aggregation].
    - Attacker chooses a point that may be detected and lost without harm.

Infiltration Phase

- Licit machines must be compromised to implement the different attacks phases.
  - Ideally in a privileged “zone” of the network, and/or
  - With access credentials, and/or
    - User credentials, address(es), hardware key, etc…
  - With “special” software, and/or
  - Target data.
- May include the installation of software or usage of licit vulnerable software.
- May be remotely controlled (constantly or not).
  - Command and control (C&C).
- May have autonomous (AI) bots installed to perform illicit actions.
  - When remote C&C is not possible or subject to easy detection.

Remotely by Exploiting Licit Users

- Objectives:
  - Credentials acquisition.
  - Software insertion.
  - Ramsomware.
- Vectors:
  - E-mail and social networking
    - Phishing for credentials.
    - Office macros.
    - Binaries execution.
  - Downloadable software
    - Cracks.
    - Non-certified software stores.
    - …



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [redacted]

I PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

Remotely by Attacker Actions

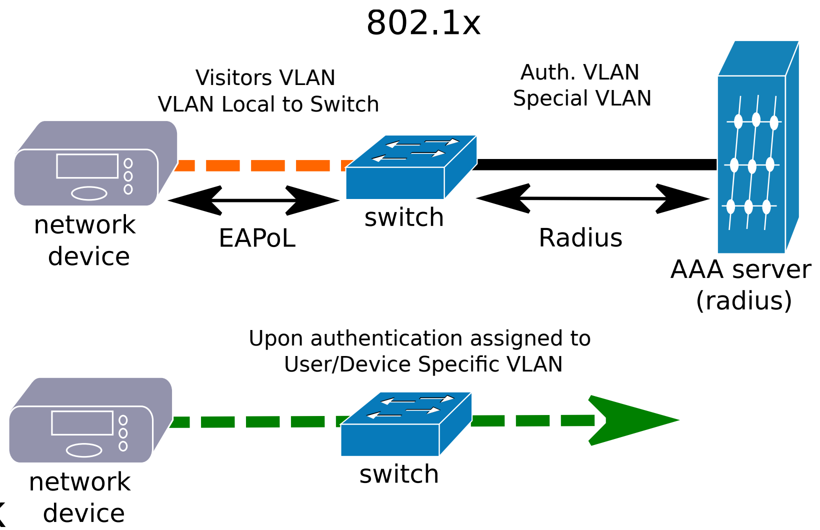
- Possible when network/systems have unpatched (unresolved) vulnerabilities.
  - Limited in time.
- Possible when network/systems are poorly configured/designed
  - Less limited in time.
  - Hard to perform discovery without detection by traditional defense systems.
    - Sometimes poorly configured/designed systems are not protected by adequate systems (if any).
- Usually not done first.
- Done after acquiring some credentials/privileges from licit users.
  - Using direct connections/services.
  - Easier to hide (stealth attacks) by having reduce activity or mimicking licit usage.

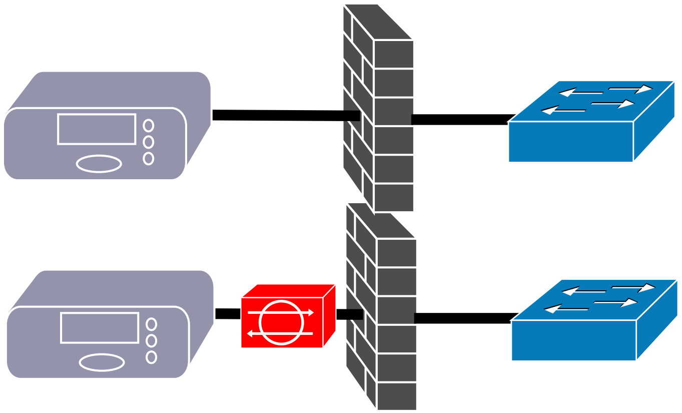
Locally by Physical Interaction

- Objectives:
  - Traffic interception.
  - Local network access to exploit vulnerabilities.
  - Direct access to machine.
- Vectors:
  - Ethernet ports at public/unprotected locations
    - With VLAN separation
    - Without VLAN separation
    - Protected by 802.1X
  - Network taps at public/unprotected locations
  - Fake access points.
    - Rogue access points
  - Network devices access
    - Unprotected serial/console ports, USB ports, etc...
  - USB ports (short time access)
    - Long time objectives
      - Trojan/root kits injection.
    - Short time objectives
      - Device data acquisition (contacts, messages, sms, etc...)
  - Sitting down at a terminal or with a device!
  - Other?

Illicit usage of Ethernet ports

- Common protection:
  - VLAN separation/isolation.
  - 802.1X.
- Unused ports
  - VLAN separation/isolation and/or 802.1x may be enough to mitigate more dangerous attacks (L2 or L3 access to internal machines).
  - Switches MAC flooding attacks and Network overload (Local DoS) are possible.
- In use ports
  - Using an inline device it is possible to break 802.1X using terminal/user authentication.
    - Traffic pass-through.
    - After 802.1X authentication performs inline MAC spoofing.
  - Allows for traffic snooping, injection, and MITM attacks.





Network Tapping

- Switch rogue mirror ports.
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Constant monitoring of configuration changes on network devices.
- Ethernet cable tap
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Electrical variations. Maybe…?
- Optical cable tap
  - Allows for traffic snooping and injection, no MITM attacks.
  - Solution: Quantum cryptography

Wireless Attack Vectors

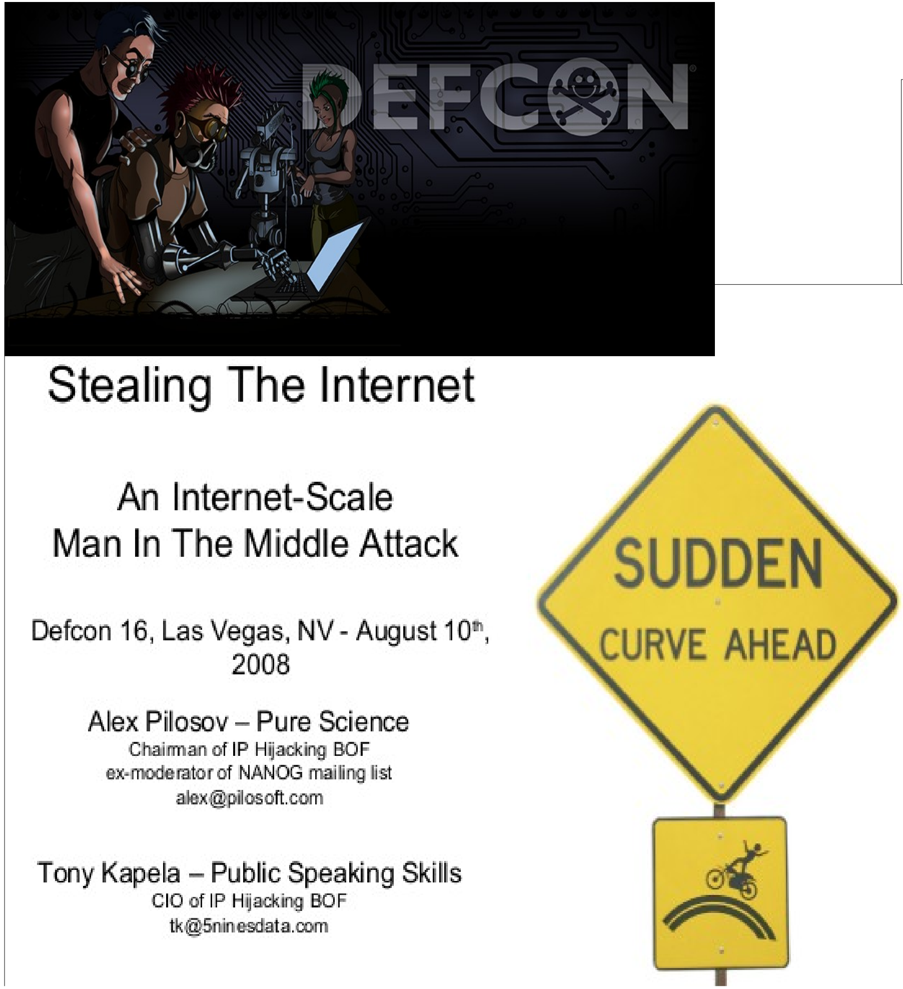
- Rogue APs
  - WPA PSK and WPA2 PSK are not compromised.
    - Unless device associates to networks with (fake) SSID of known networks with different credentials and/or secure protocols.
      - Decision to connect based only on stored SSID and not other parameters.
  - WPA Enterprise and WPA2 Enterprise security may be compromised on 2nd phase authentication.
    - Credentials not recoverable (maybe with MSCHAPv2).
    - Permits “accept everyone” strategy for MITM attacks.
  - Open+Web-based authentication are very vulnerable.
    - Fake entry portals.
  - Allows DoS.
    - Force user to search other networks. Make user choose insecure/fake network.
- Wireless Interception (possible injection).
- Electromagnetic effects
  - Wireless mouses, keyboards, …
    - Solution: additional information to scramble data.
- By Sound
  - Keystrokes sounds.

E300 electromagnetic field intensity analyzer

The host of E300

www.shutterstock.com · 70646725

BGP & Internet-Scale Traffic Redirection Attack (2008)


DEFCON
SUDDEN
CURVE AHEAD

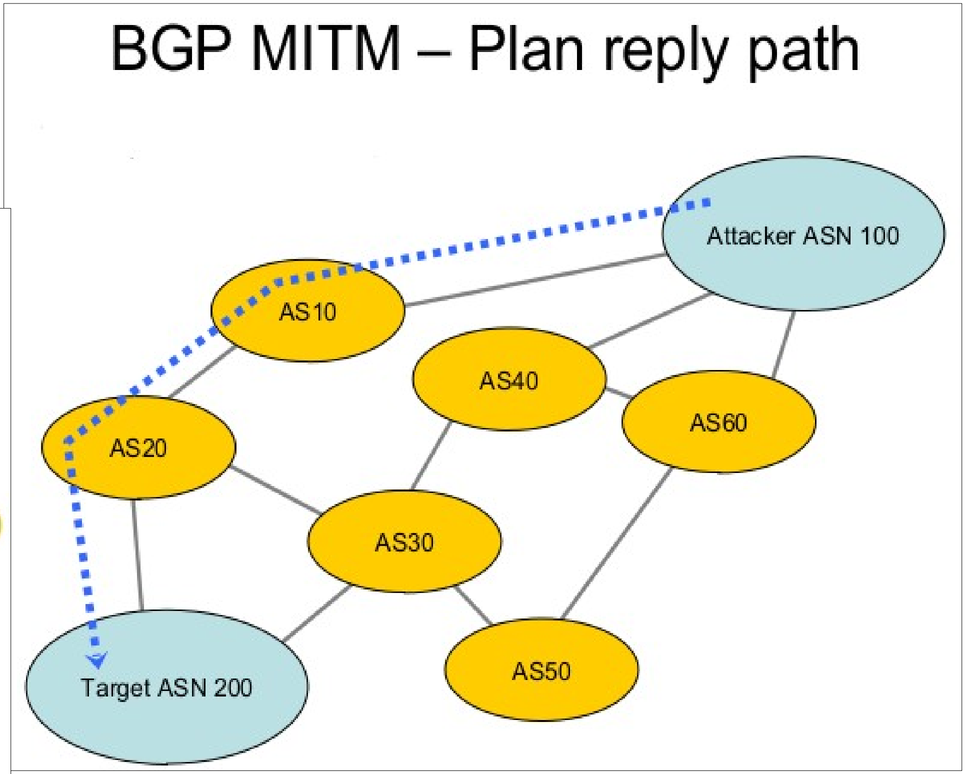
Stealing The Internet

An Internet-Scale
Man In The Middle Attack

Defcon 16, Las Vegas, NV - August 10th, 2008

Alex Pilosov – Pure Science
Chairman of IP Hijacking BOF
ex-moderator of NANOG mailing list
alex@pilosoft.com

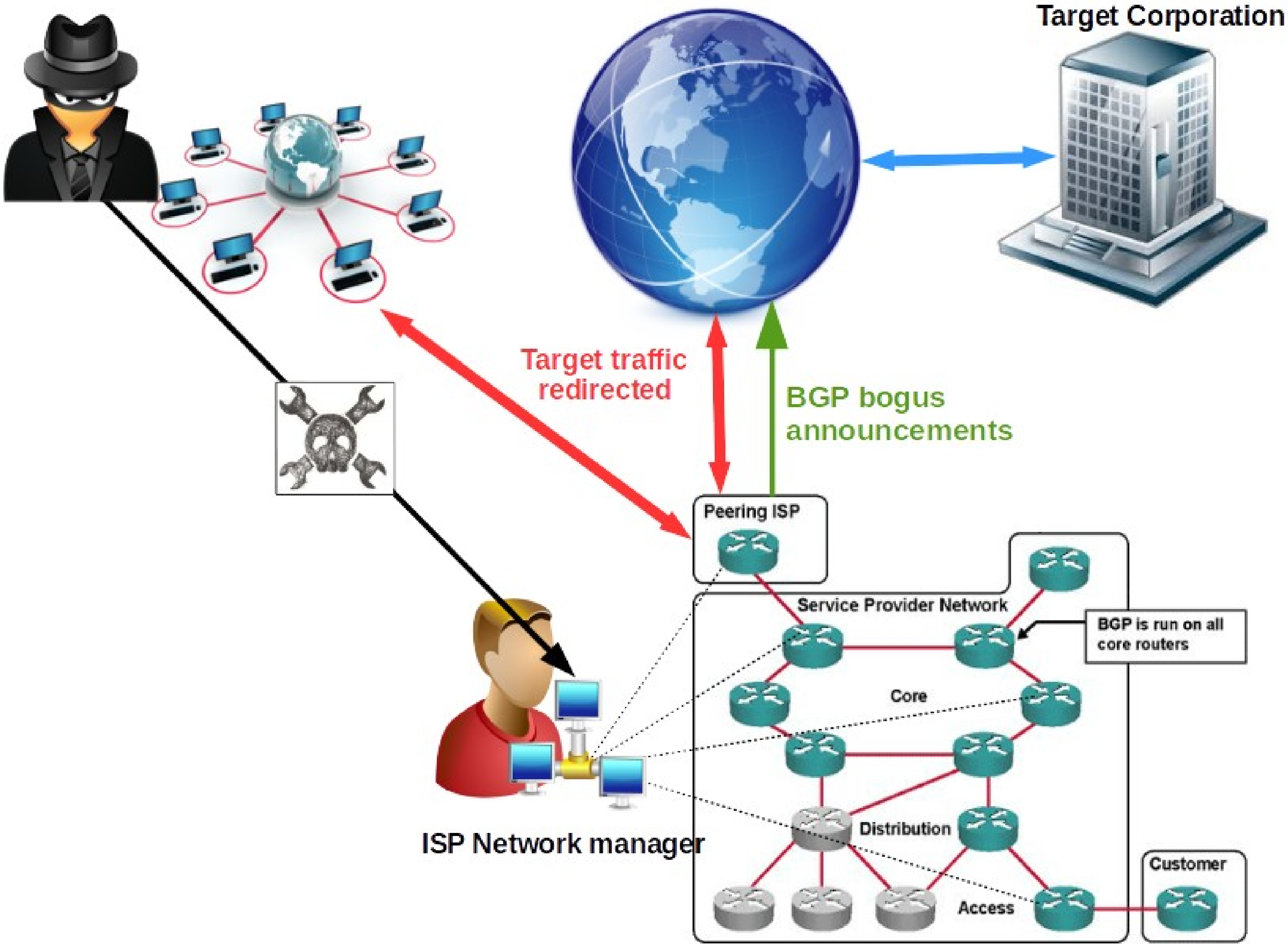
Tony Kapela – Public Speaking Skills
CIO of IP Hijacking BOF
tk@5ninesdata.com



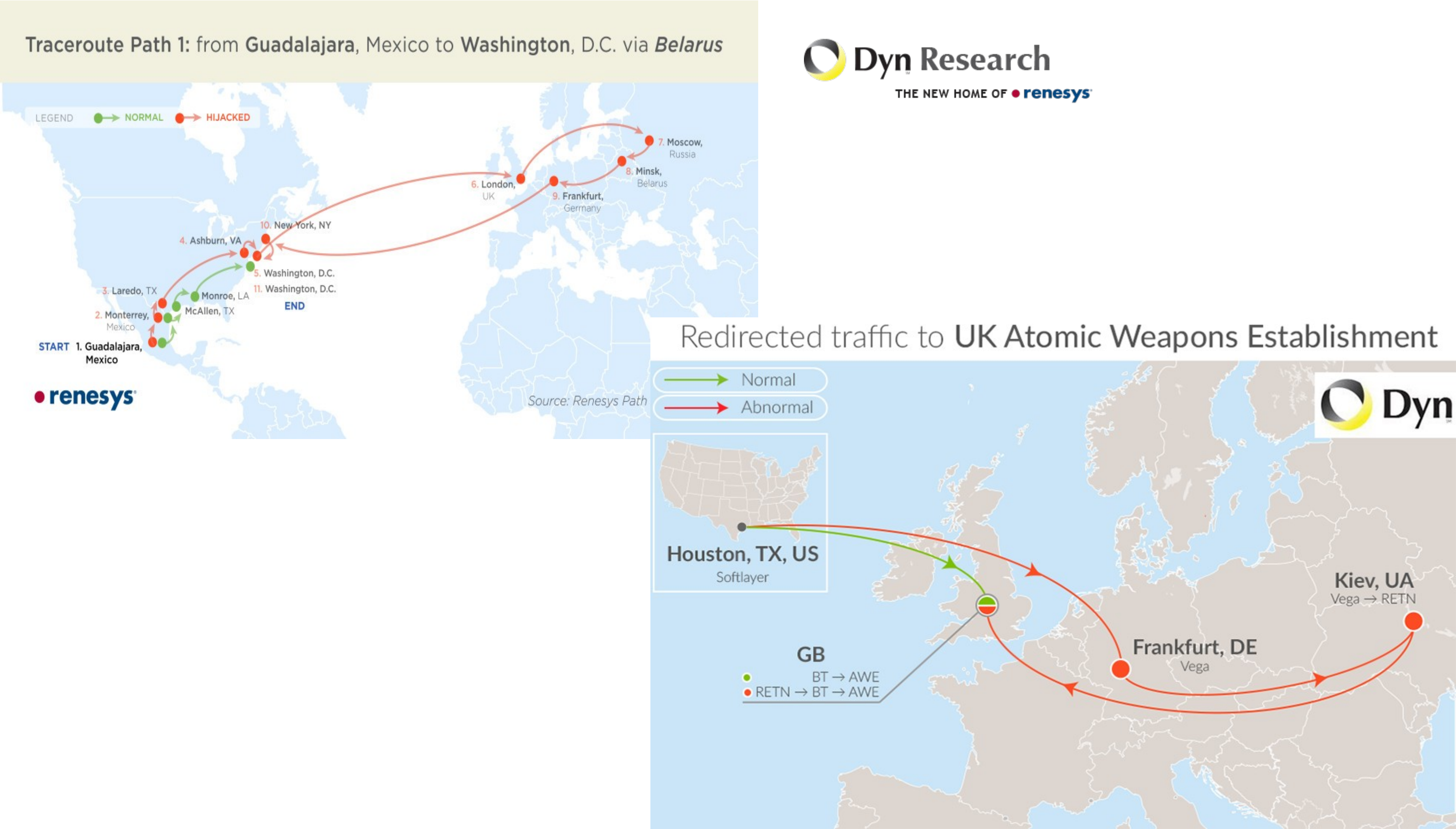
BGP MITM – Plan reply path

http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

MP-BGP Attack Vector



Latest (known/public) Reports



Traceroute Path 1: from **Guadalajara**, Mexico to **Washington**, D.C. via ***Belarus***

Redirected traffic to **UK Atomic Weapons Establishment**

http://dyn.com/blog/uk-traffic-diverted-ukraine/

Propagation Phase

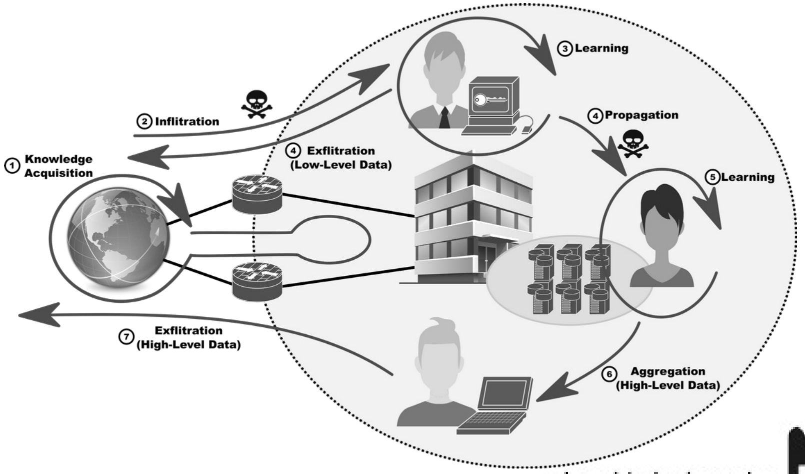
- Done using a mixture of methodologies:
  - Credentials exploitation.
    - Direct usage or by using allowed applications.
  - Impersonating users and systems.
    - Similar to credential exploitation but more advanced based on acquired knowledge (licit behavior).
    - Requires time to learn and mimic licit behavior.
      - Time patterns, traffic patterns, application patterns, etc...
  - Vulnerability exploitation.
    - Inside a protected domain systems are many times considered in a secure zone.
    - Less maintained and legacy OS/applications may be required to run (no patching).
    - Broader range of vulnerabilities

Aggregation and Exfiltration Phase

- Data transferred from machine to machine.
- Internally [Aggregation] it can be done using existing channels.
- Externally [Exfiltration]
  - It can be done directly using existing channels.
    - File copy, email, file sharing, etc…
    - Can be detected.
  - It can be done hiding information within existing/allowed channels and licit communications.
    - Slower data transfer, harder (impossible?) to detect.
    - Examples:
      - Usage of steganography in photos (via social networking).
      - Usage of embed data in text and voice messages.
      - ...

Challenges

- Traditional network/systems defenses cannot guarantee total security of machines.
- Cannot prevent infiltration.
  - User Liberty vs. Data Confidentiality vs. Security equilibrium.
  - New threats/methodologies are almost impossible to prevent.
- A network manager must assume that any machine may be compromised at any time.
- Solution:
  - Monitor network and systems to prevent more damaging actions from/in compromised machines.
  - Detect attack in more important phases:
    - Network Propagation,
    - Network Aggregation,
    - Data Exfiltration (Most Important!).



1 Knowledge Acquisition
2 Infiltration
3 Learning
4 Exfiltration (Low-Level Data)
4 Propagation
5 Learning
6 Aggregation (High-Level Data)
7 Exfiltration (High-Level Data)

Security News and Events

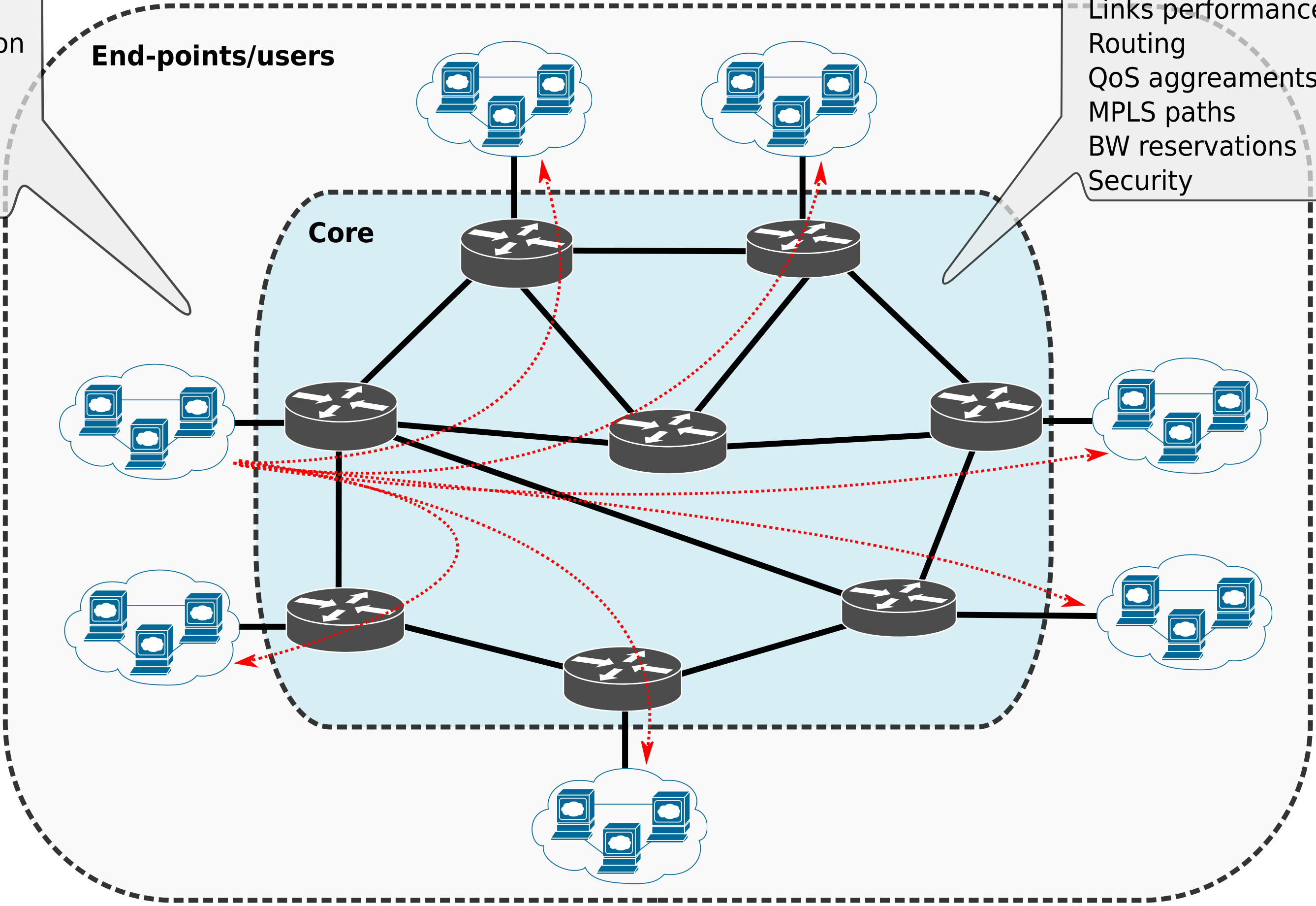
- www.bleepingcomputer.com
- www.securityboulevard.com
- www.threatpost.com
- www.reddit.com/r/security/
- www.reddit.com/r/cybersecurity/

Data Acquisition

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 aggreaments
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

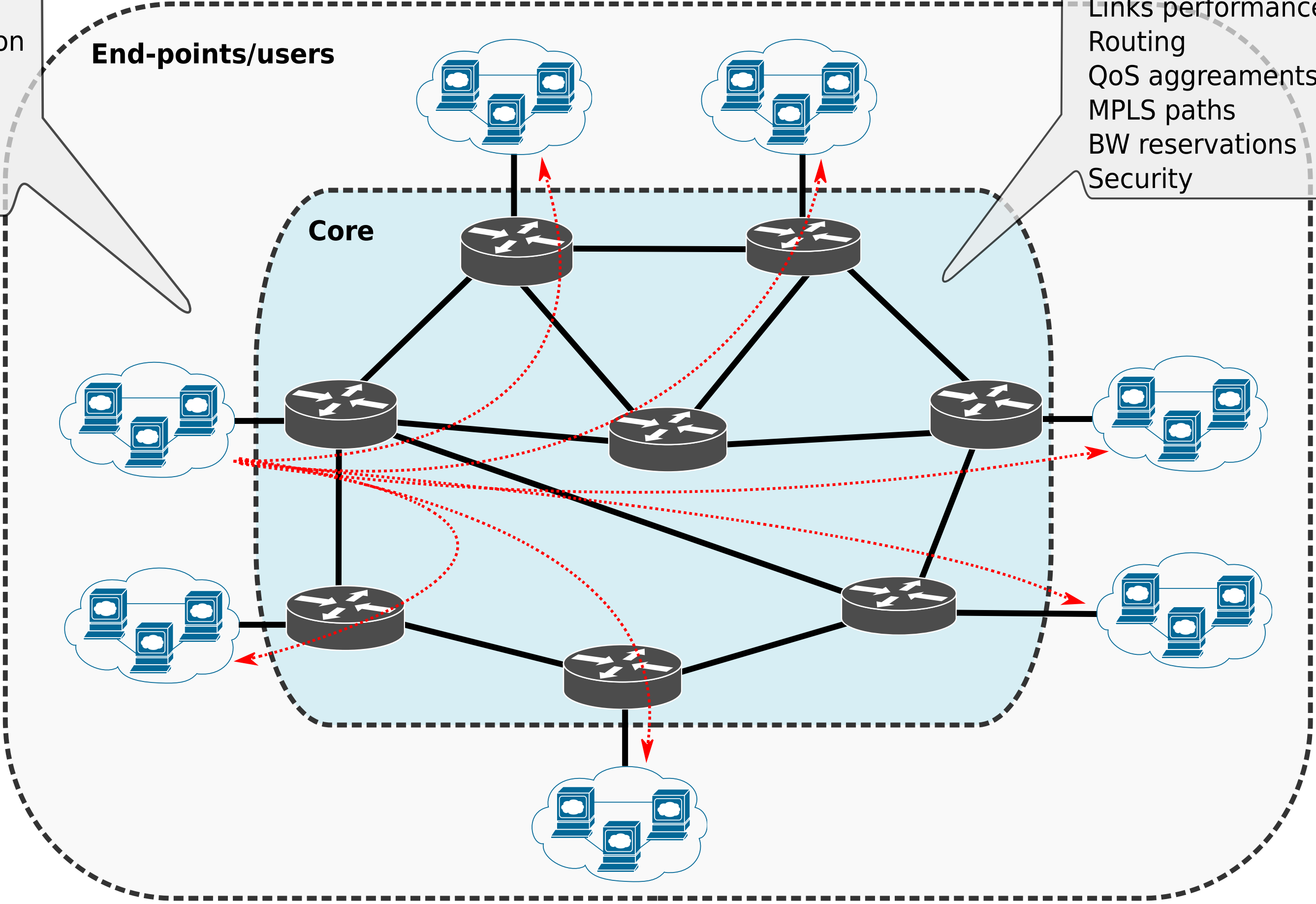
Routing

QoS aggreaments

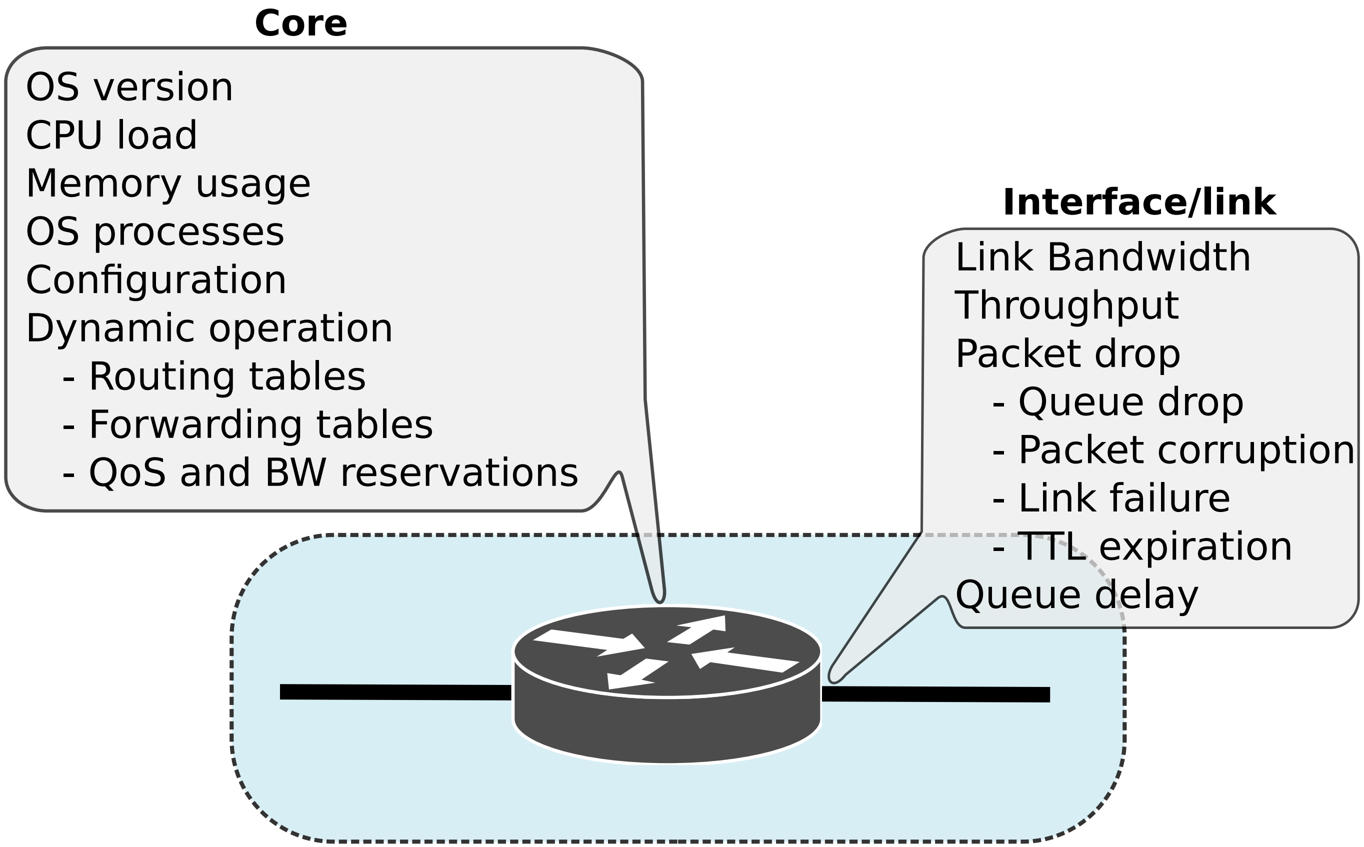
MPLS paths

BW reservations

Security



Node Monitoring



Core

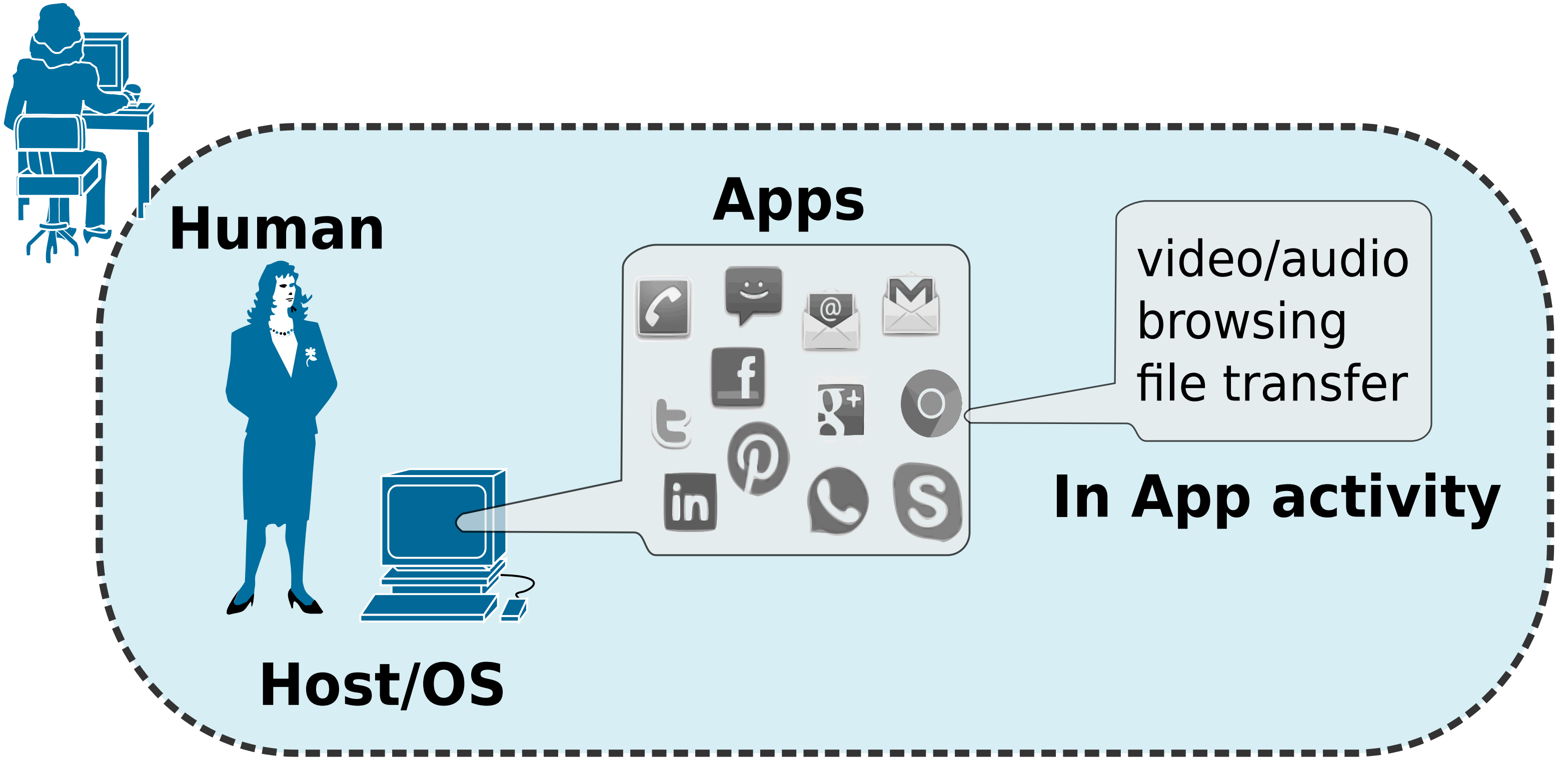
OS version
CPU load
Memory usage
OS processes
Configuration
Dynamic operation
- Routing tables
- Forwarding tables
- QoS and BW reservations

Interface/link

Link Bandwidth
Throughput
Packet drop
- Queue drop
- Packet corruption
- Link failure
- TTL expiration

Queue delay

End-User/Host/App Monitoring



Server/Service/Cloud Monitoring

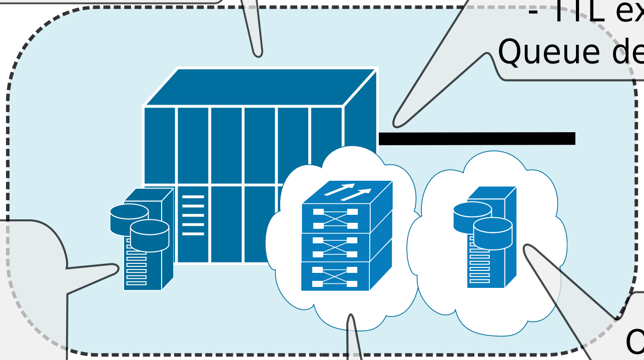
Physical Hardware

OS versions
CPU loads
Memory usages
Temperature
Power consuption
Virtualization Info.

Physical Network

Link Bandwidth
Throughput
Packet drop
- Queue drop
- Packet corruption
- Link failure
- TTL expiration

Queue delay



OS version
CPU load
Memory usage
OS processes
Configurations
Service performace
Service errors

Physical Server/Service

Link Bandwidth
Throughput
Packet drop
- Queue drop
- Packet corruption
- Link failure
- TTL expiration

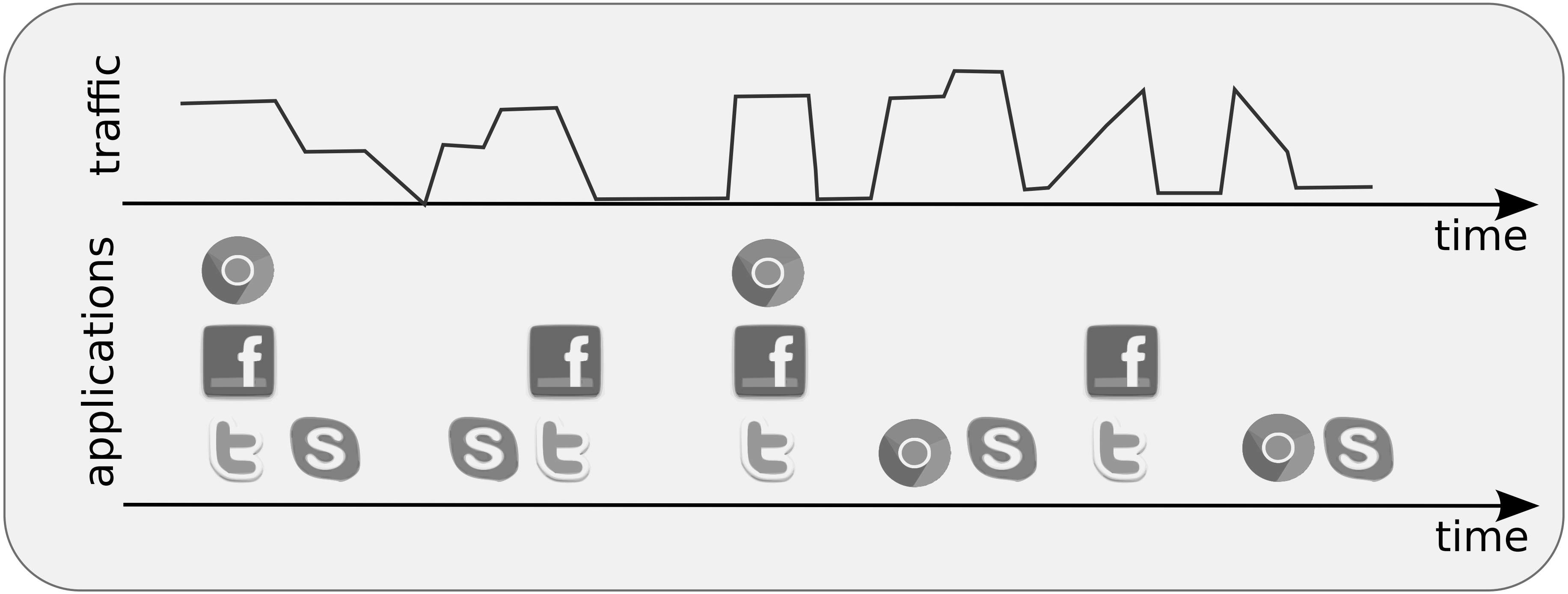
Queue delay

Virtual Networks

OS version
CPU load
Memory usage
OS processes
Configurations
Service performace
Service errors

Virtual Servers/Services

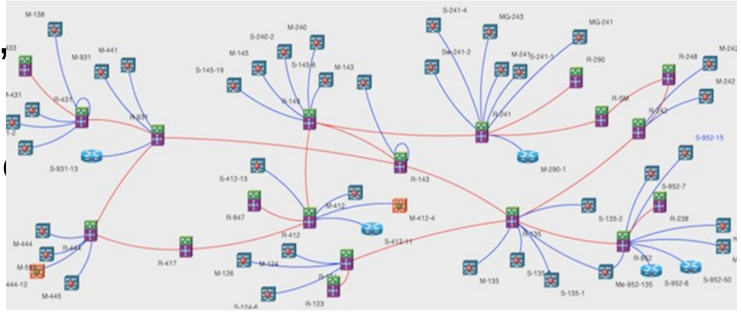
Overtime Monitoring



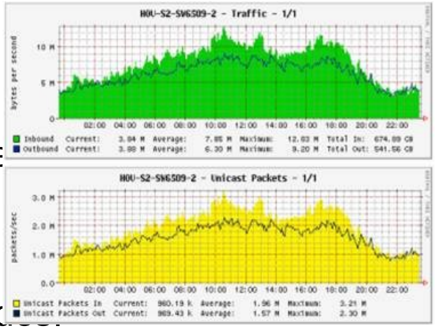
Data Sources

- 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

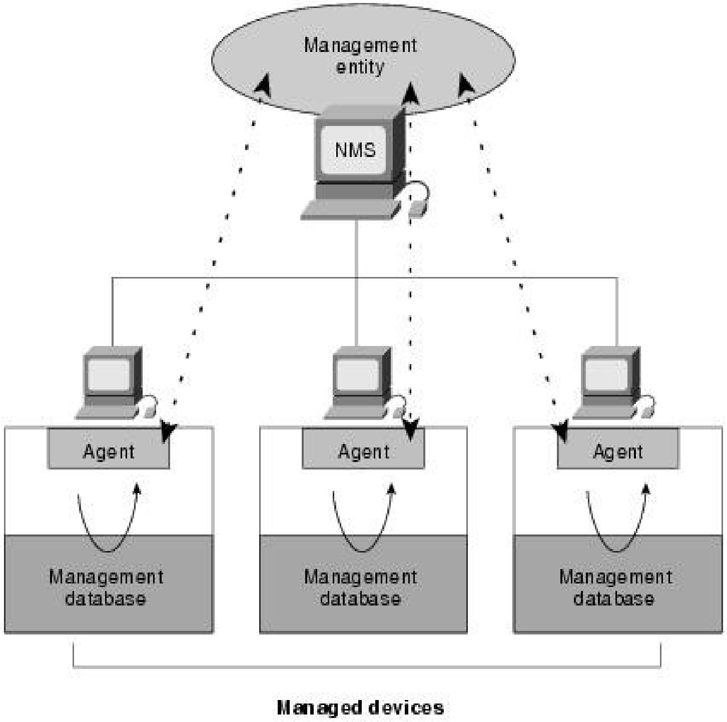


- Used for acquiring the status and usage of nodes, links and services over time.
  - Requires periodic pulling to obtain information over tim
- Used for obtain:
  - Network elements and interconnections,
  - Network deployed services.
- Used for estimating, characterizing, and predict:
  - Data flow performance.
    - Packet losses and (by indirect inference) delay/jitter at nodes.
    - Allows to obtain information about current and future service performance
  - Nodes performance,
    - Memory/CPU usage, number of processes, etc...
    - Allows to detect points of failure, service degradation nodes, unstable nod
  - 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.

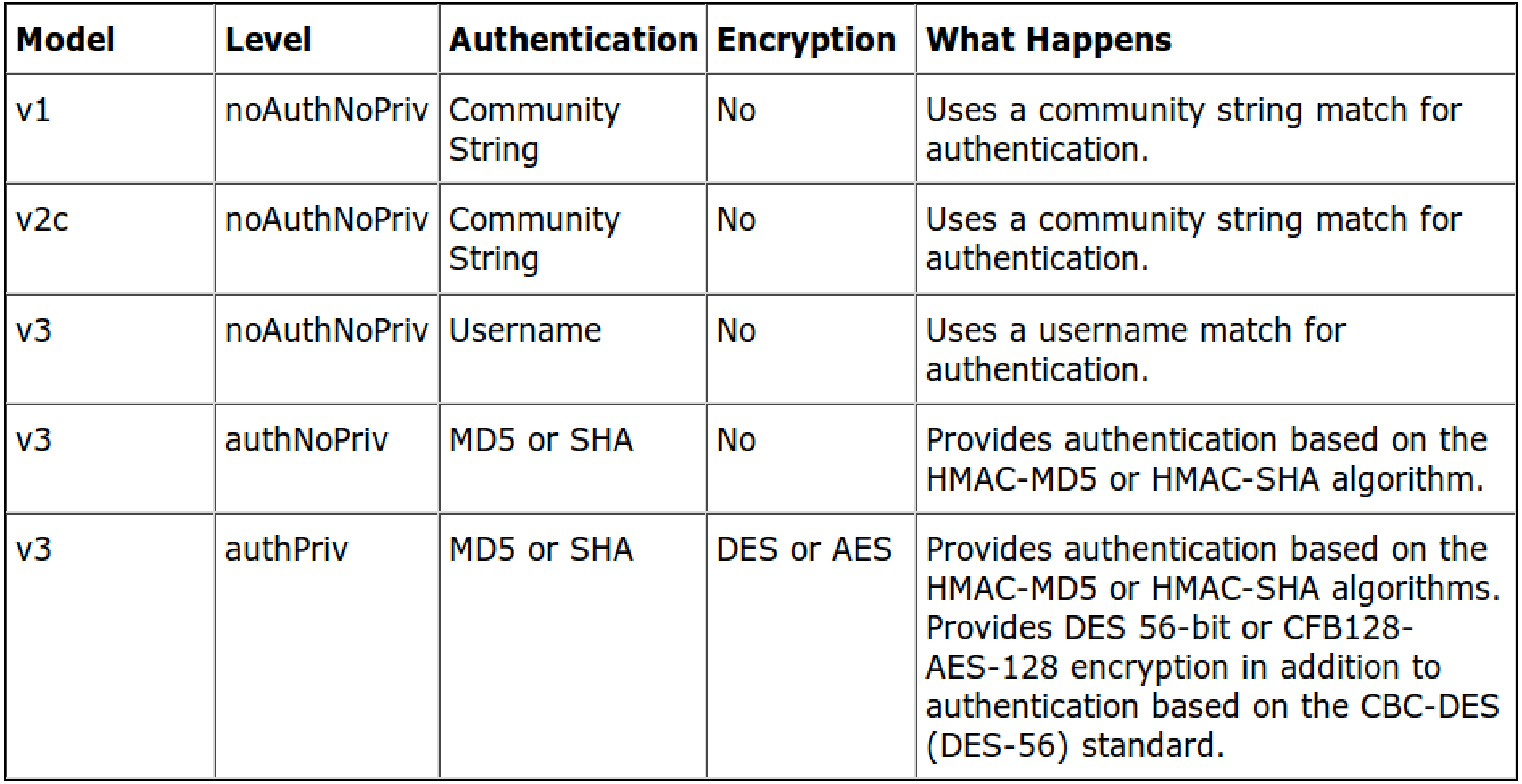


SNMP Basic Components

- 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.



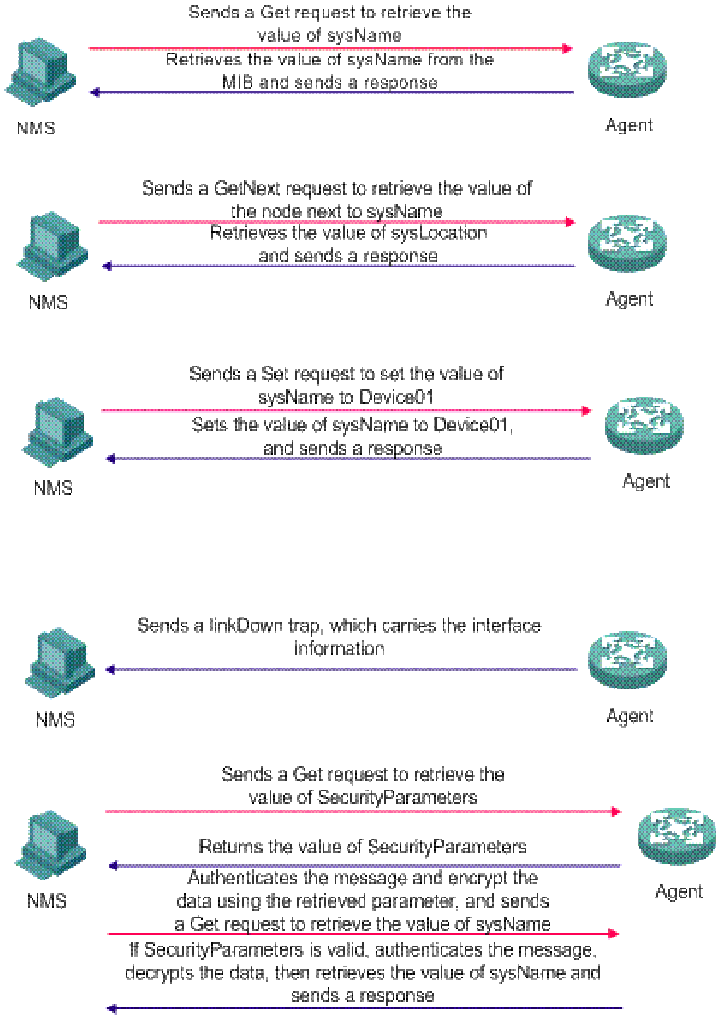
SNMP Versions



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.



Sends a Get request to retrieve the value of sysName

Retrieves the value of sysName from the MIB and sends a response

Sends a GetNext request to retrieve the value of the node next to sysName

Retrieves the value of sysLocation and sends a response

Sends a Set request to set the value of sysName to Device01

Sets the value of sysName to Device01, and sends a response

Sends a linkDown trap, which carries the interface information

Sends a Get request to retrieve the value of SecurityParameters

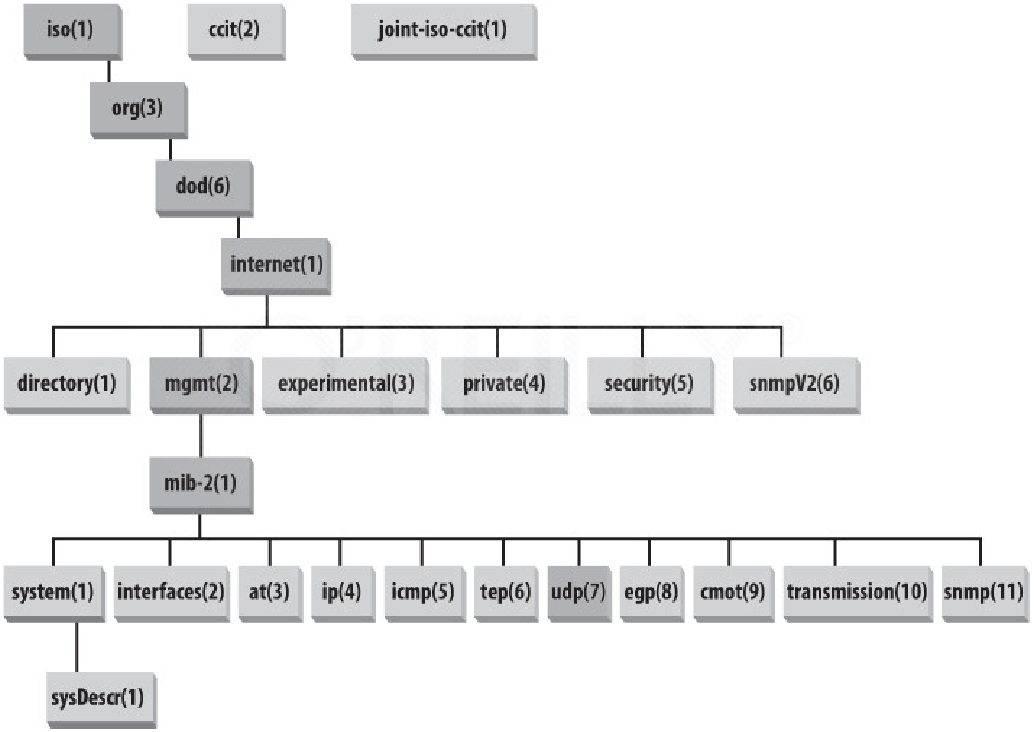
Returns the value of SecurityParameters

Authenticates the message and encrypt the data using the retrieved parameter, and sends a Get request to retrieve the value of sysName

If SecurityParameters is valid, authenticates the message, decrypts the data, then retrieves the value of sysName and sends a response

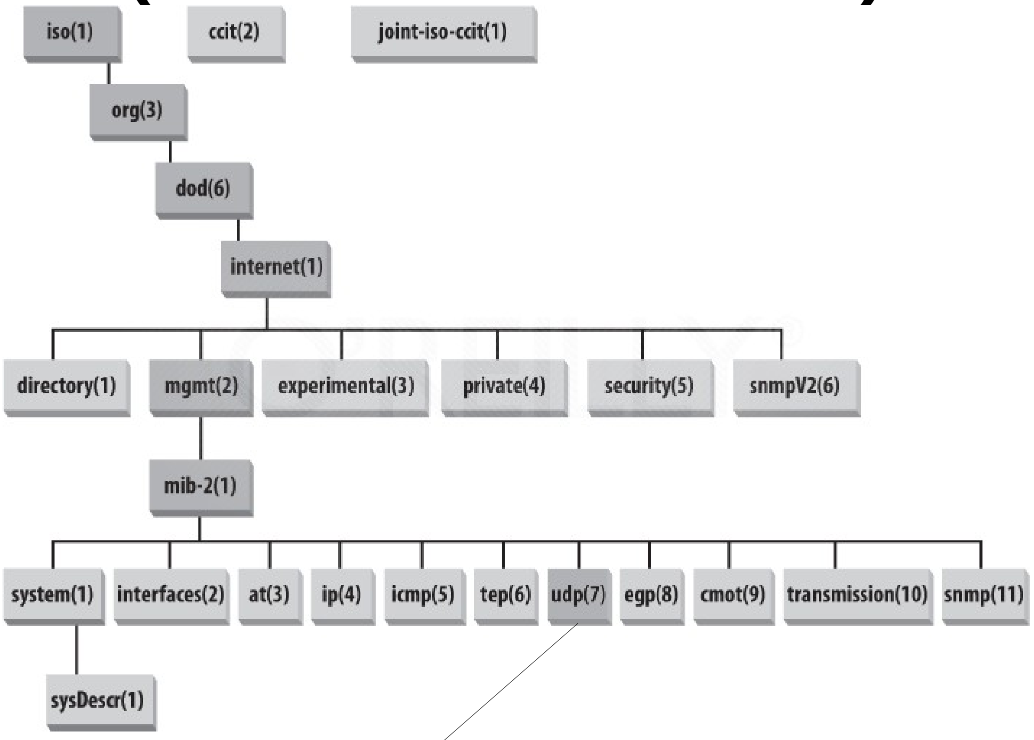
MIB Modules and Object Identifiers

- 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



1.3.6.1.2.1.7.1

ISO
ISO-ident. Org.
US DoD
Internet

udpInDatagrams
UDP
MIB2
management

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

IP header	UDP header	NetFlow header	NetFlow record	...	NetFlow record

Header format

Version 1

byte 3	byte 2	byte 1	byte 0
version		count	
system uptime			
UNIX seconds			
UNIX nanoseconds			

Version 5

byte 3	byte 2	byte 1	byte 0
version		count	
system uptime			
UNIX seconds			
UNIX nanoseconds			
flow sequence number			
engine type	engine ID	reserved	

Record format

Version 1

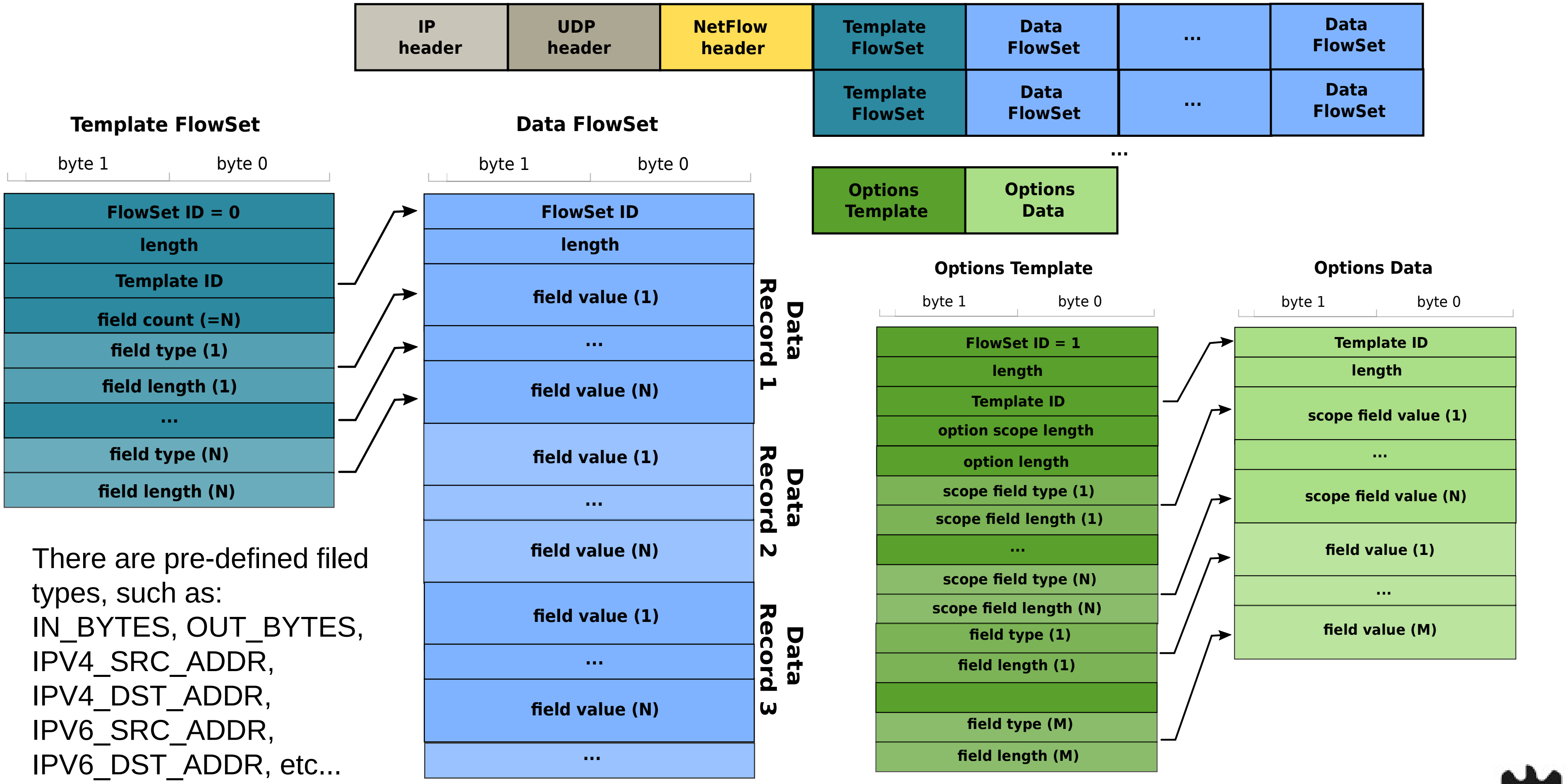
byte 3	byte 2	byte 1	byte 0
source IP address			
destination IP address			
next-hop IP address			
input interface index		output interface index	
packets			
bytes			
start time of flow			
end time of flow			
source port		destination port	
pad		IP protocol	TOS
TCP flags	padding		
reserved			

Version 5

byte 3	byte 2	byte 1	byte 0
source IP address			
destination IP address			
next-hop IP address			
input interface index		output interface index	
packets			
bytes			
start time of flow			
end time of flow			
source port		destination port	
pad	TCP flags	IP protocol	TOS
source AS		destination AS	
src netmask length	dst netmask length	pad	

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...

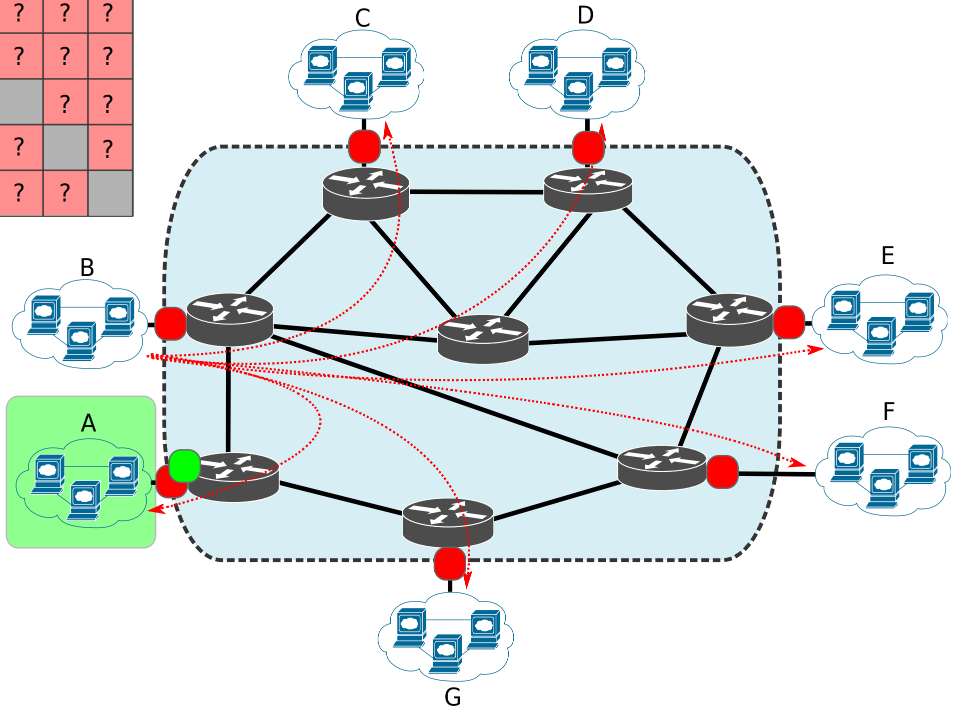
NetFlow Usage

- 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

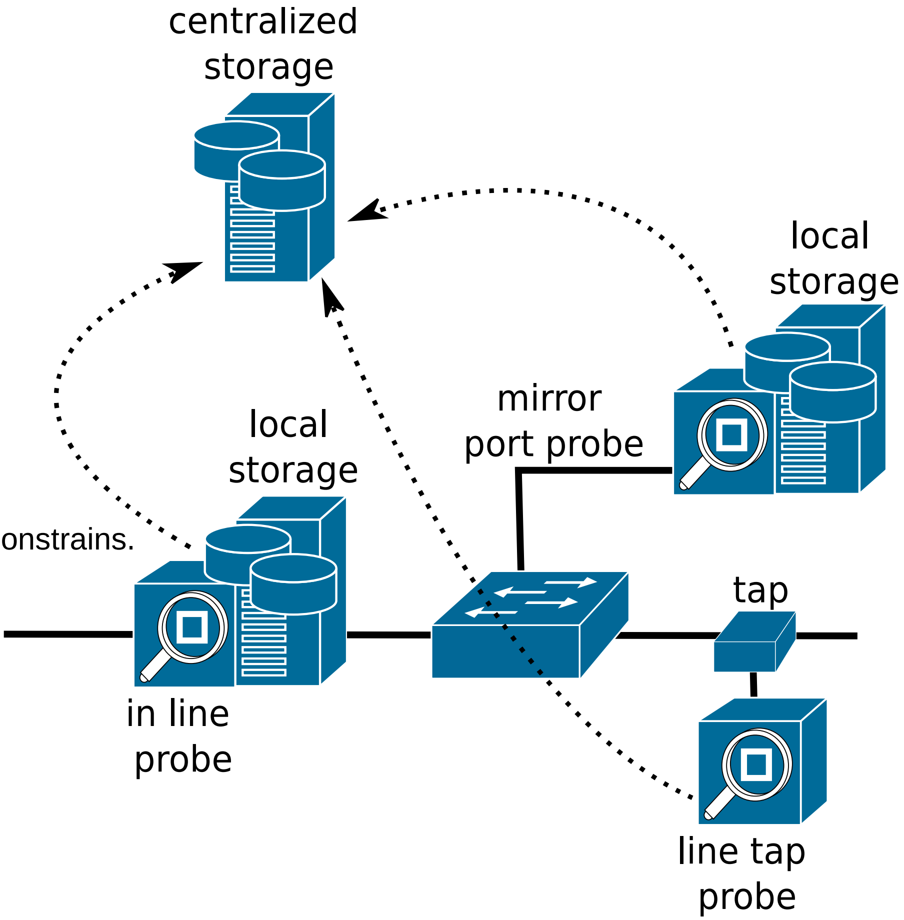
- IPFIX is very similar to NetFlow v9
  - Uses version 10 in a similar header.
  - Also has Templates and Data Records.
  - Also has Options Templates and Options Data Records.
- IPFIX made provisions for NetFlow v9 and added support for it.
  - IPFIX lists an overview of the “Information Element identifiers” 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.

sFlow and jFlow

- sFlow
  - Uses sampling techniques designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.
  - Allow monitoring network traffic at Gigabit speeds and higher.
  - Allow to scale the monitoring of tens of thousands of agents from a single sFlow collector.
  - Supported by multiple vendors.
    - Including Cisco in
- jFlow is used in Juniper equipments.
  - Similar to NetFlow, however version 9 it also allows the usage of flow sampling techniques

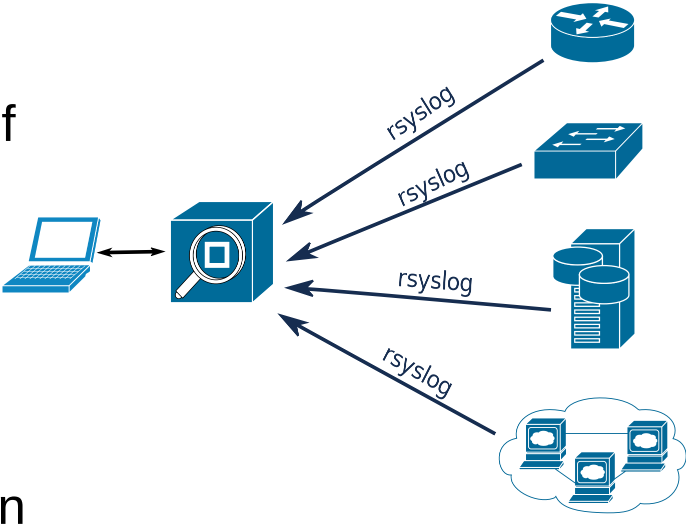
Network Passive Probing
Packet Capturing

- User for:
  - Specific and detailed data inference,
  - Infer small and medium timescale dynamics.
- Probe types
  - Switch mirror port,
  - In-line,
  - Network tap.
- 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.

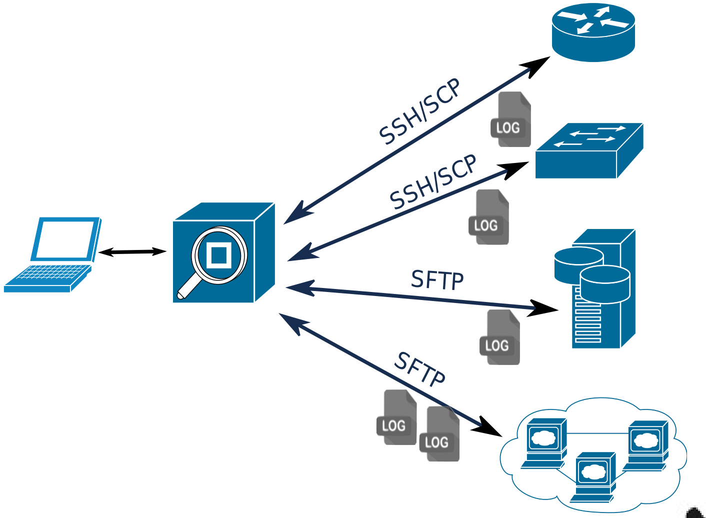


Log Files Access

- 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.

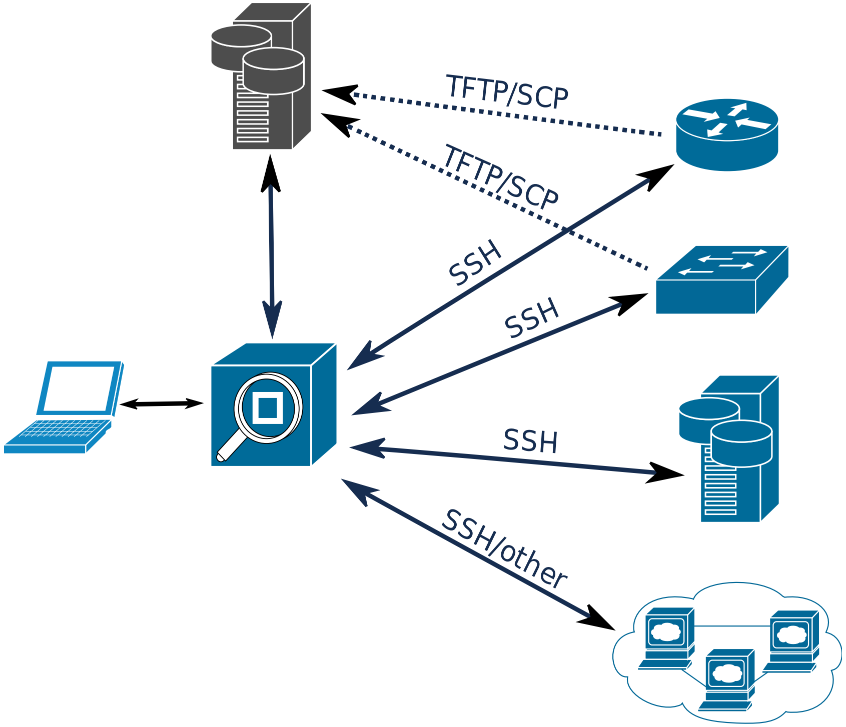


- Direct access to log files
  - Using any remote access to remote files.
    - Requires special permissions.
  - SSH/SCP, SFTP, etc...
  - Timing controlled by central point.
  - Requires all heavy post- and cross-processing in a central point.



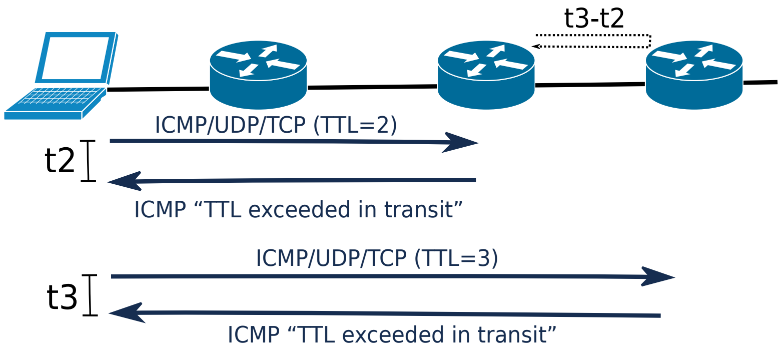
Remote CLI Access

- 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.



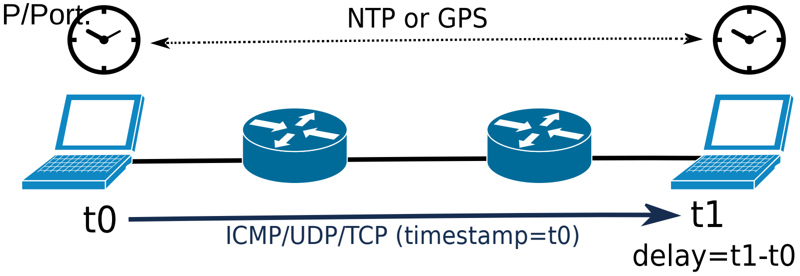
Active Measurements

- Two-way delay/jitter
  - End-to-end and middle hop.
  - Requires the control of only one end.
  - Ping and traceroute like solutions.
    - Requires that middle nodes respond to probes.
      - ICMP “TTL exceeded in transit” message.
    - ICMP, UDP or TCP.
      - UDP/TCP allows to test QoS (DiffServ) by IP/Port.

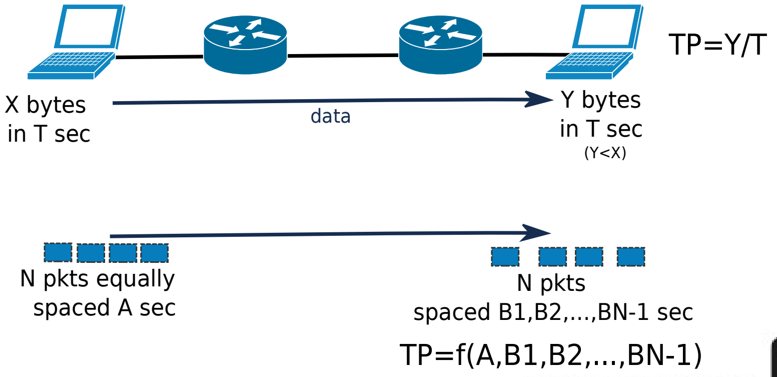


t3-t2
ICMP/UDP/TCP (TTL=2)
t2
ICMP “TTL exceeded in transit”
ICMP/UDP/TCP (TTL=3)
t3
ICMP “TTL exceeded in transit”

- One-way delay/jitter
  - End-to-end.
  - Requires control of both ends and clock synchronization.
    - May be complex/impossible for close nodes (low delay).

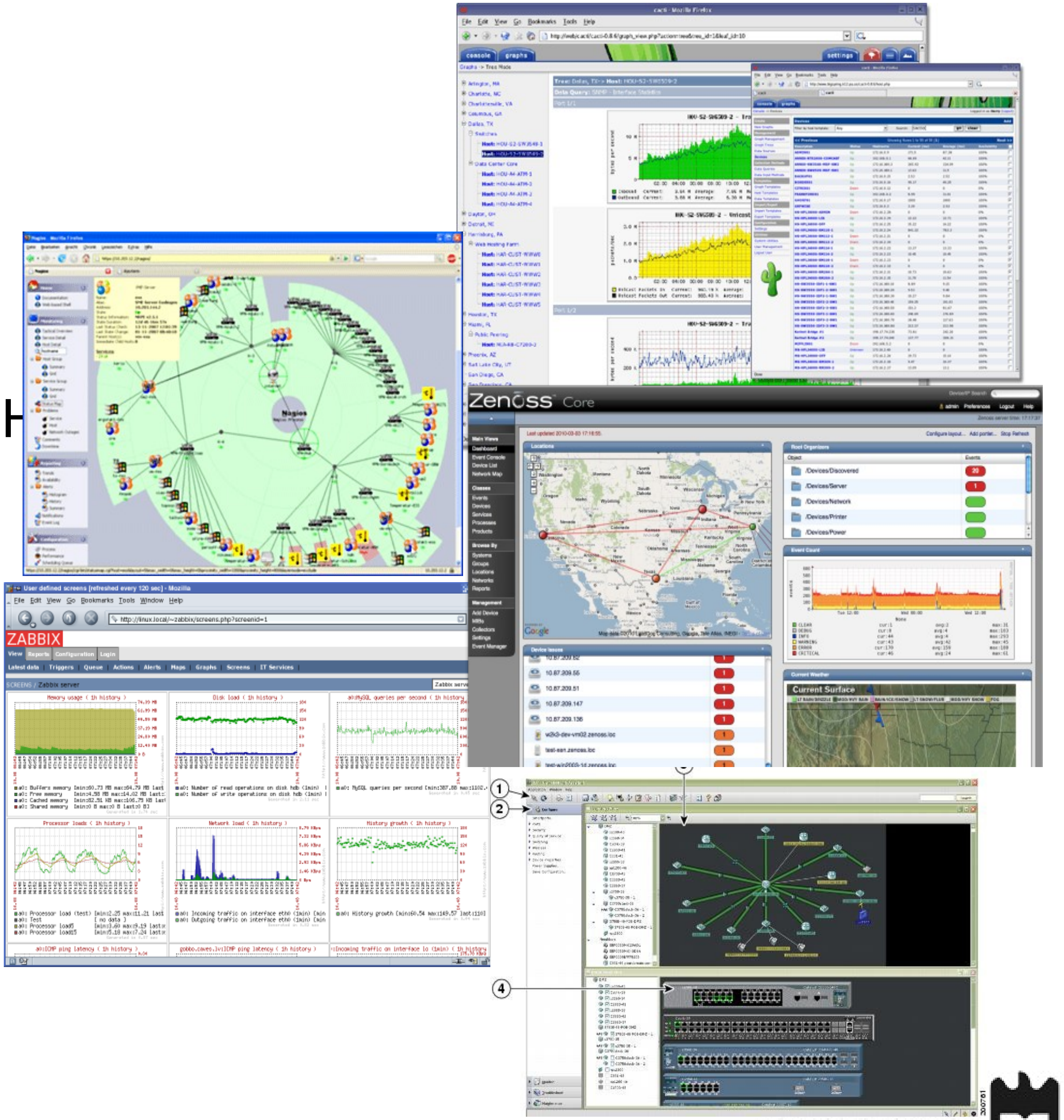


- End-to-end throughput
  - Requires control of both ends.
  - Directly sending/receiving large amounts of data.
  - Indirectly using packet train techniques.
    - Prone to errors.



Open Source/Commercial Tools

- Cacti and Cricket
  - SNMP + RRDtool graphing
- Nagios
  - SNMP + HTTP + SSH + DB + other
  - Plugins
- Zenoss
- Zabbix
- Cisco Network Assistant
- Etc...


Nagios
ZABBIX
Zenoss Core
1
2
4