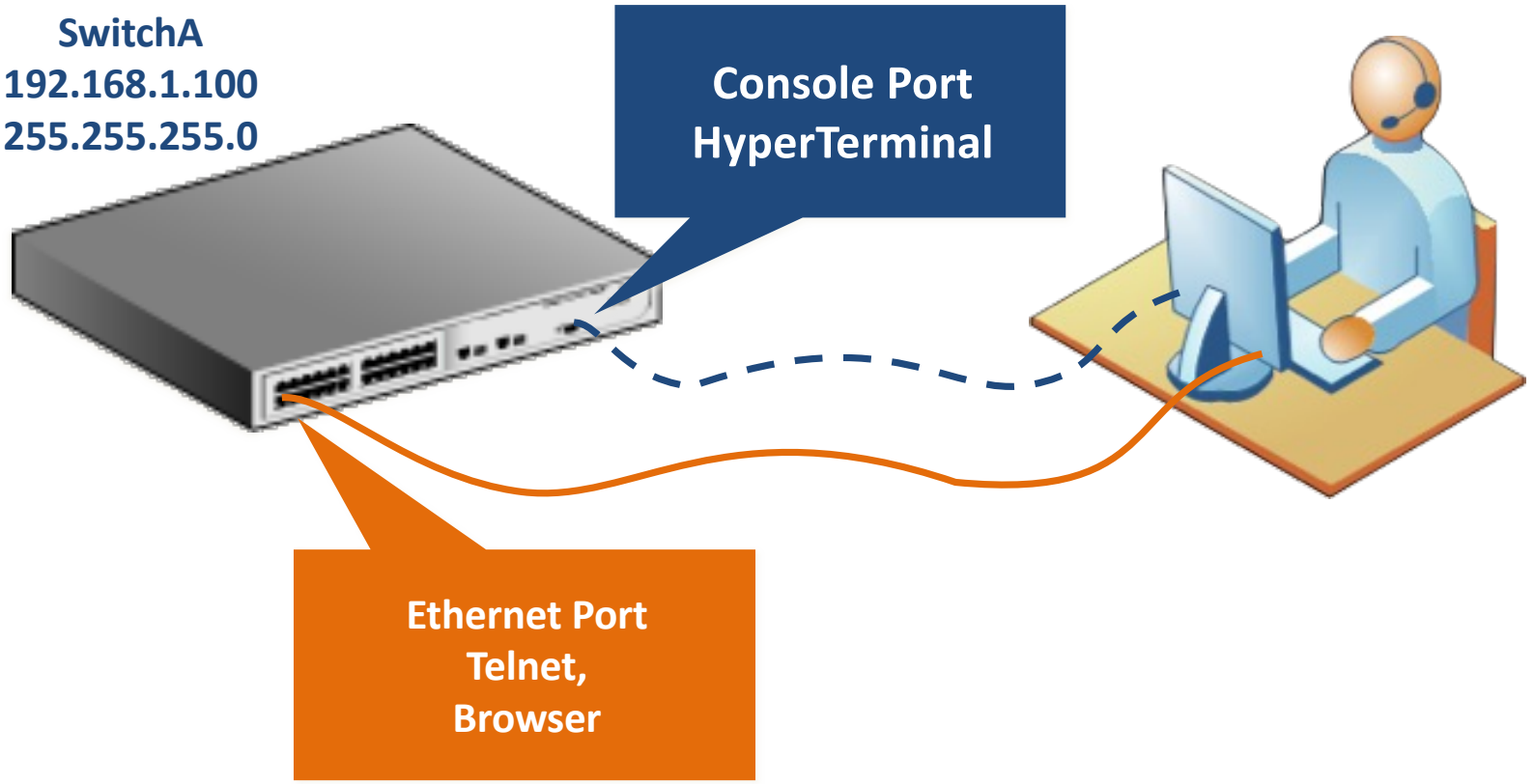
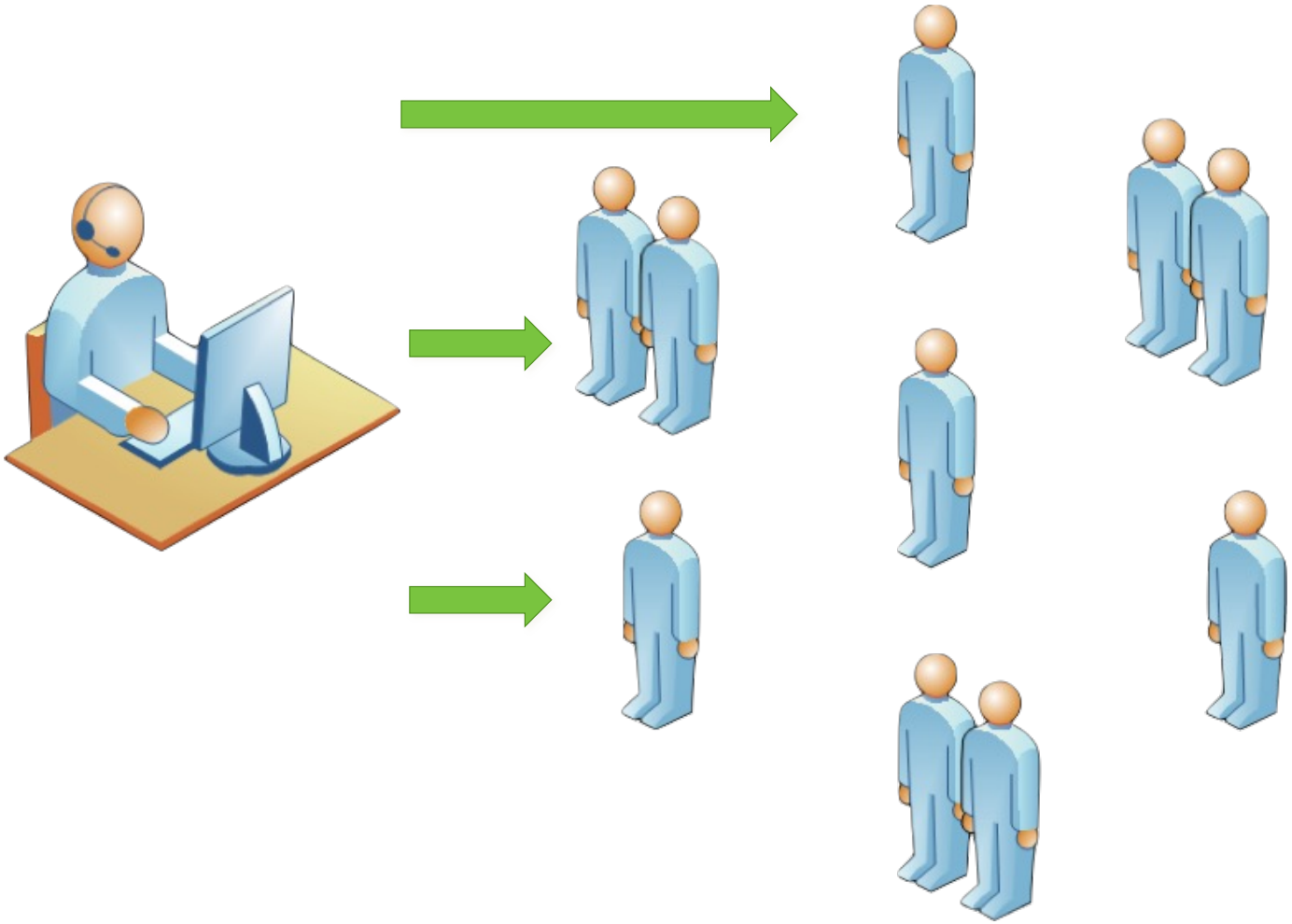
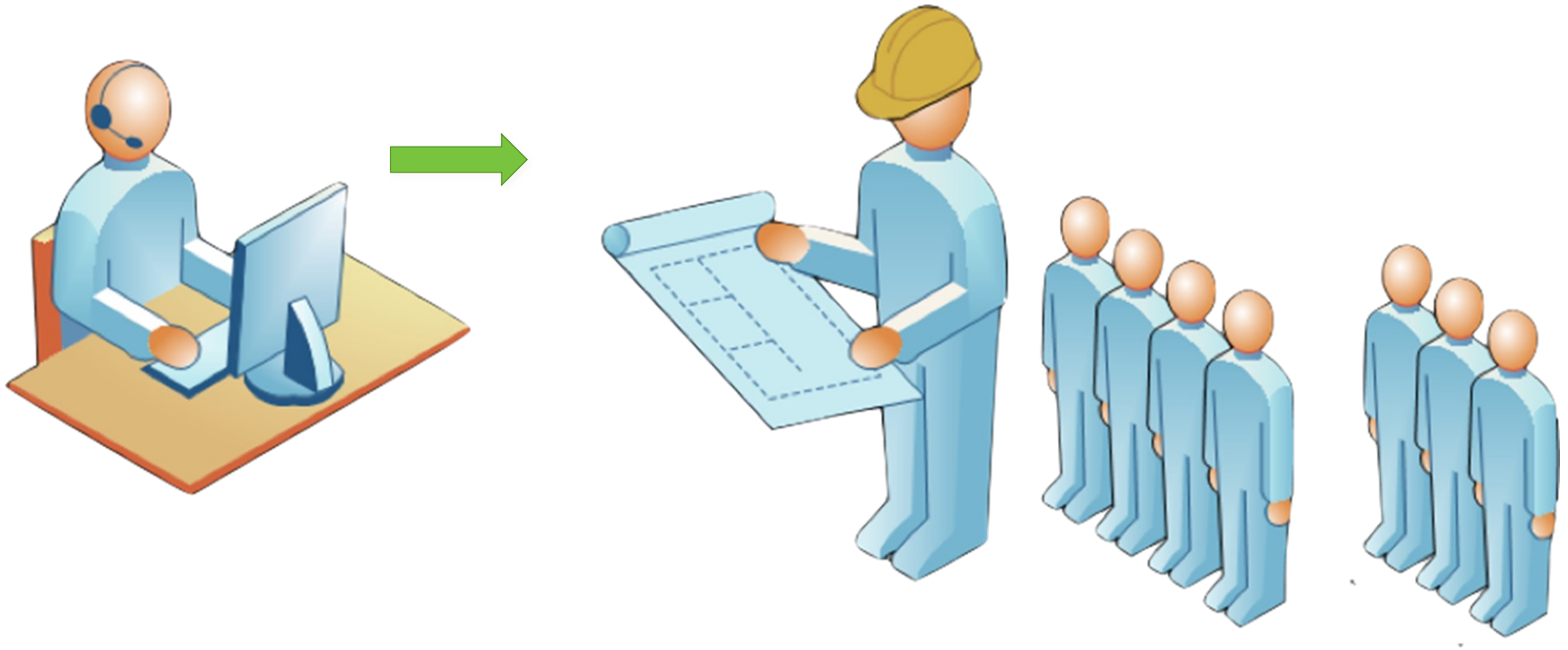
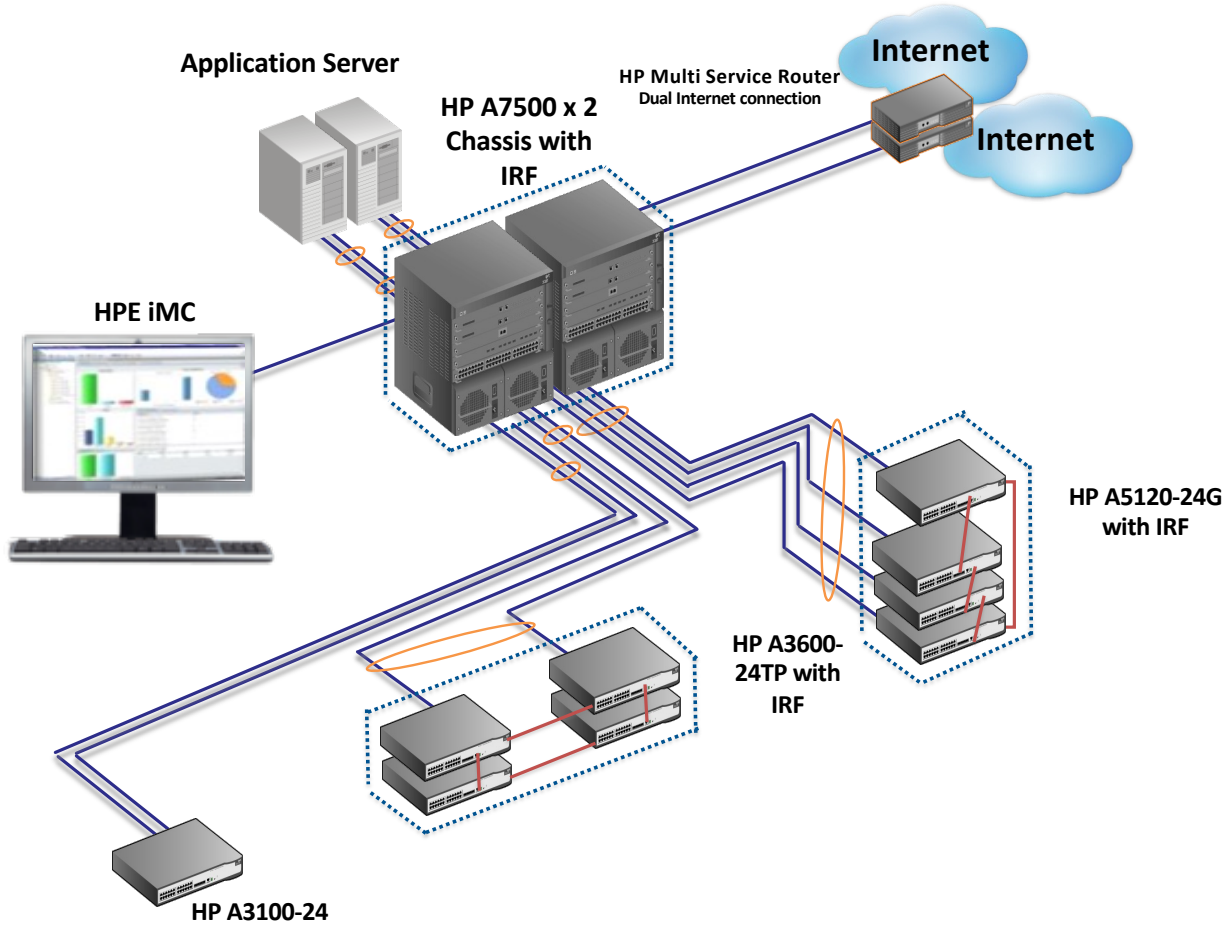
Network Management System

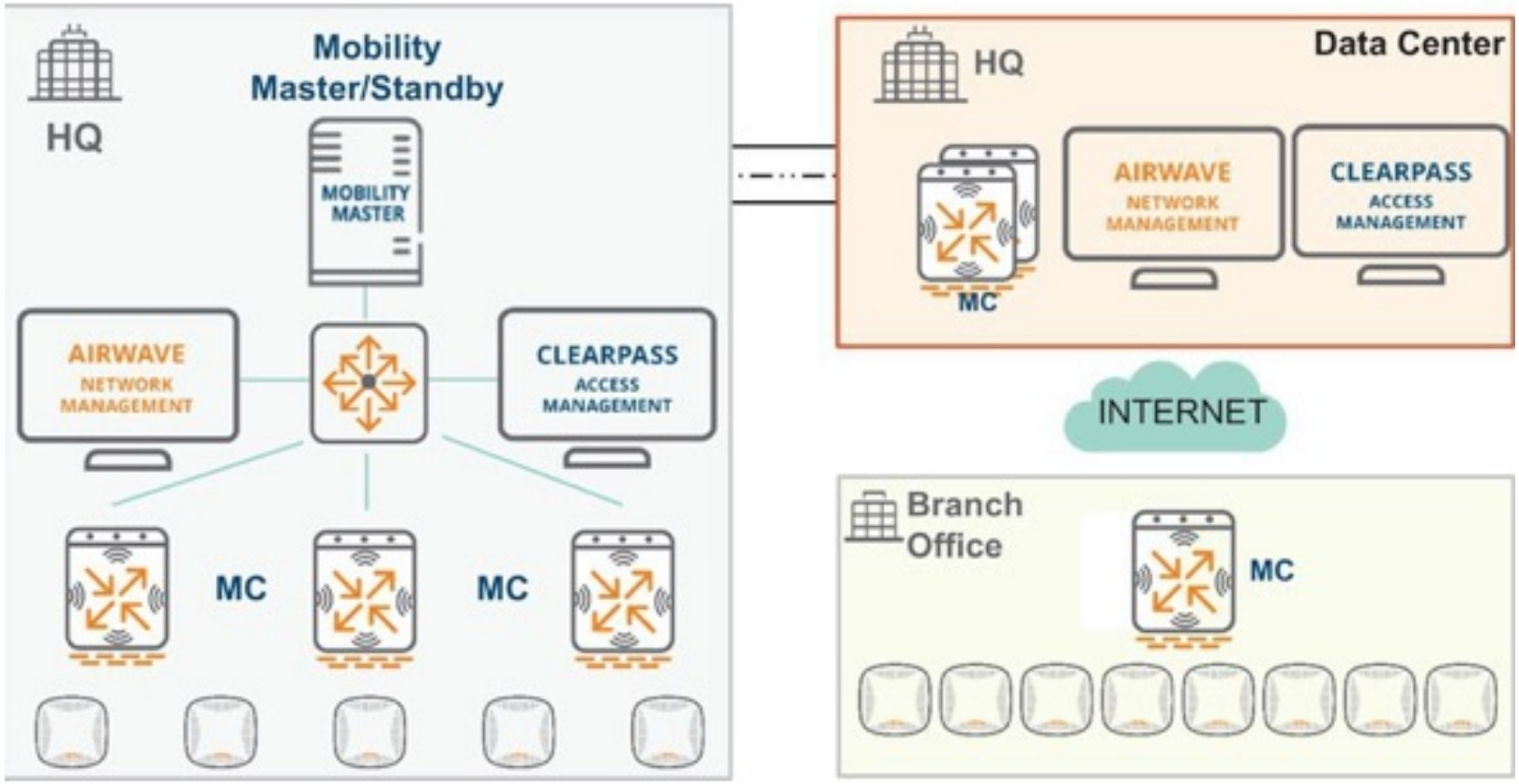
SNMP, LLDP, sFlow, NTP, SDN, REST API


SwitchA
192.168.1.100
255.255.255.0
Console Port
HyperTerminal
Ethernet Port
Telnet,
Browser






Application Server
HP A7500 x 2
Chassis with
IRF
HP Multi Service Router
Dual Internet connection
Internet
Internet
HPE iMC
HP A5120-24G
with IRF
HP A3600-
24TP with
IRF
HP A3100-24


Mobility
Master/Standby
HQ
MOBILITY
MASTER
AIRWAVE
NETWORK
MANAGEMENT
CLEARPASS
ACCESS
MANAGEMENT
MC
MC
HQ
Data Center
AIRWAVE
NETWORK
MANAGEMENT
CLEARPASS
ACCESS
MANAGEMENT
MC
INTERNET
Branch
Office
MC

NETWORK MANAGEMENT SYSTEM

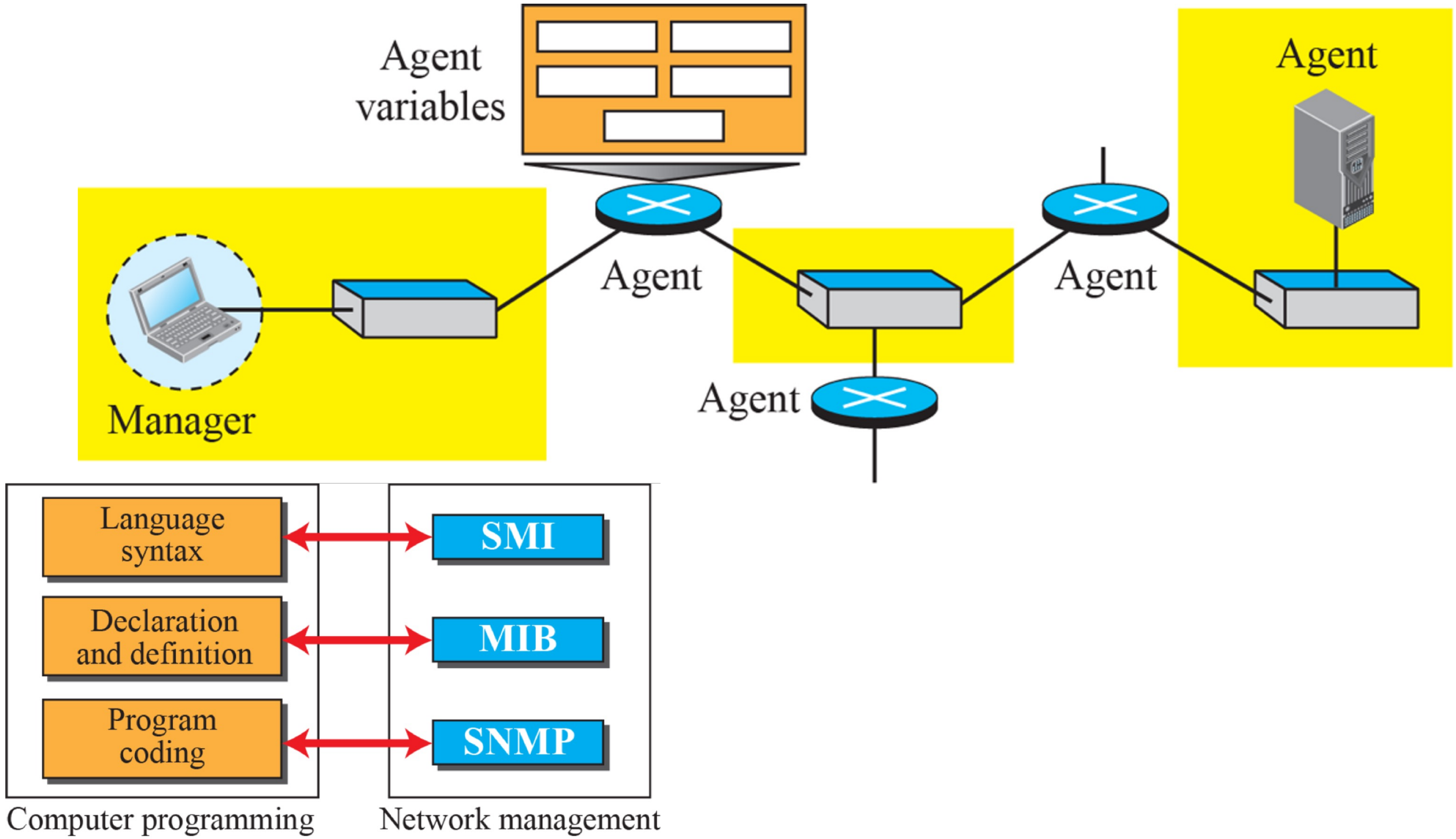
- Process and techniques of monitoring and configuring networks
- Five key areas referred to as FCAPS, under the OSI (Open System Interconnect) model :
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management

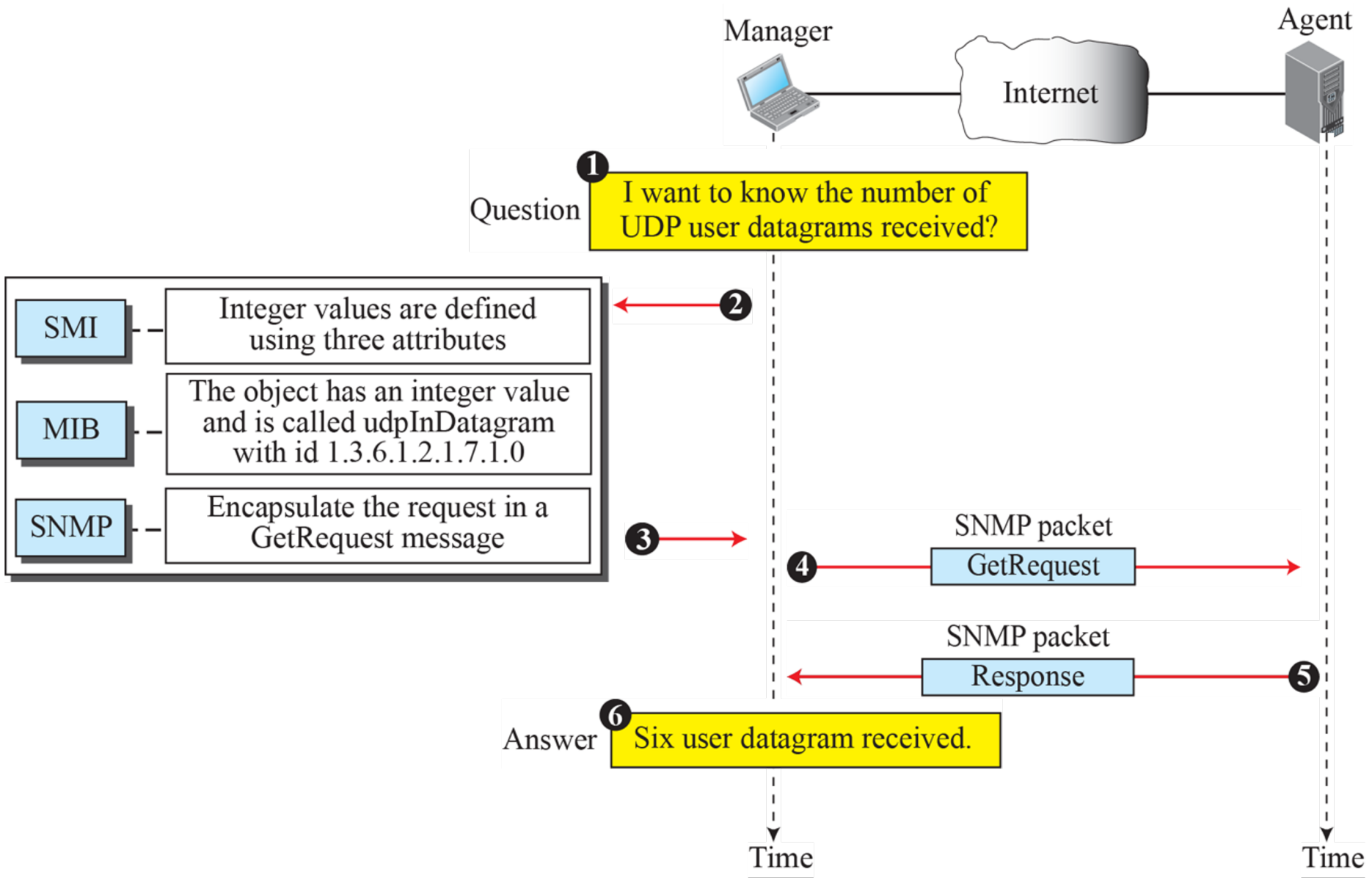
SNMP Overview

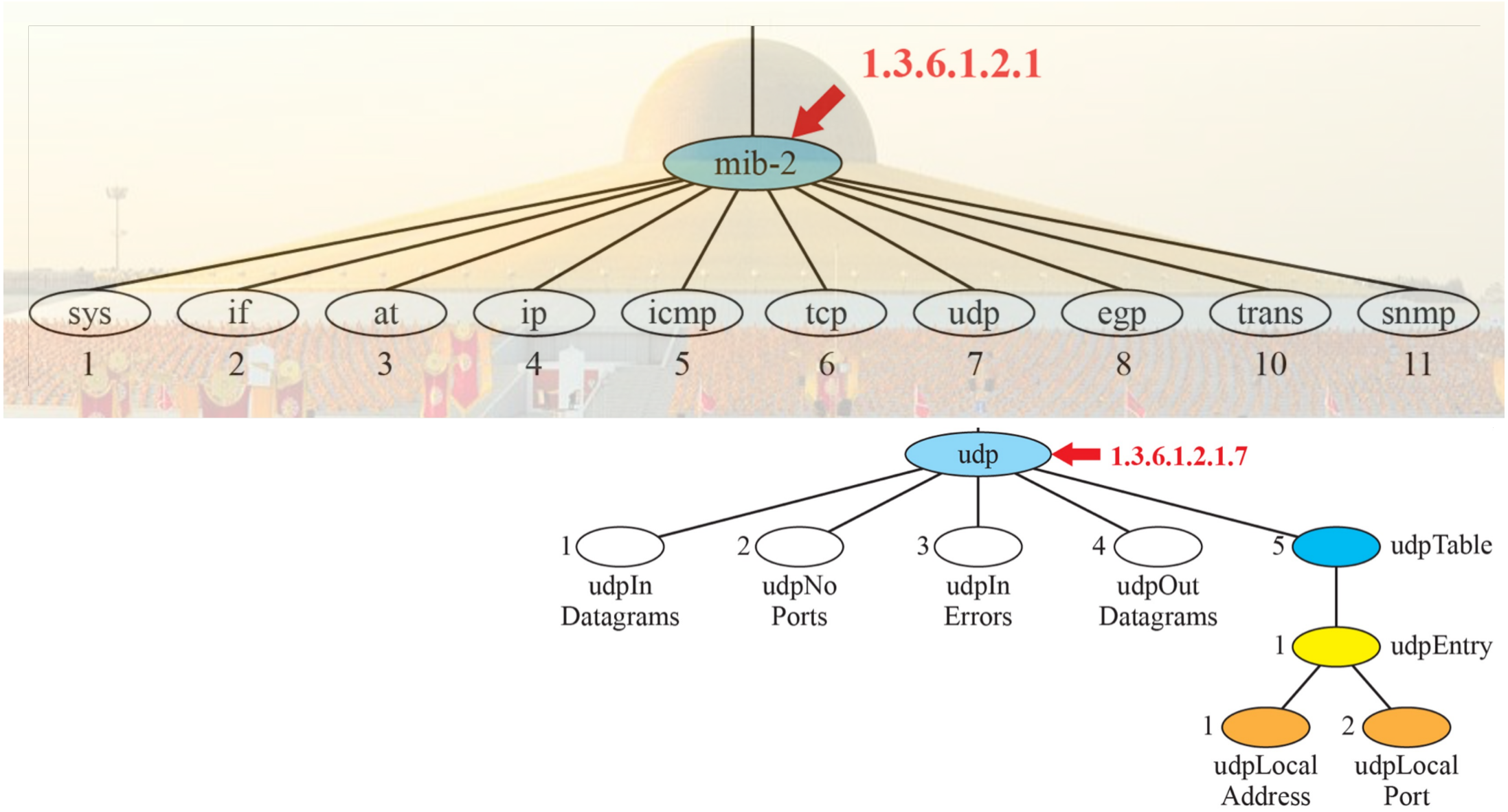
- The Simple Network Management Protocol is an Internet Standard protocol widely used for a *management station* to access and operate the *devices* on a network, regardless of their vendors and interconnect technologies.
- SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

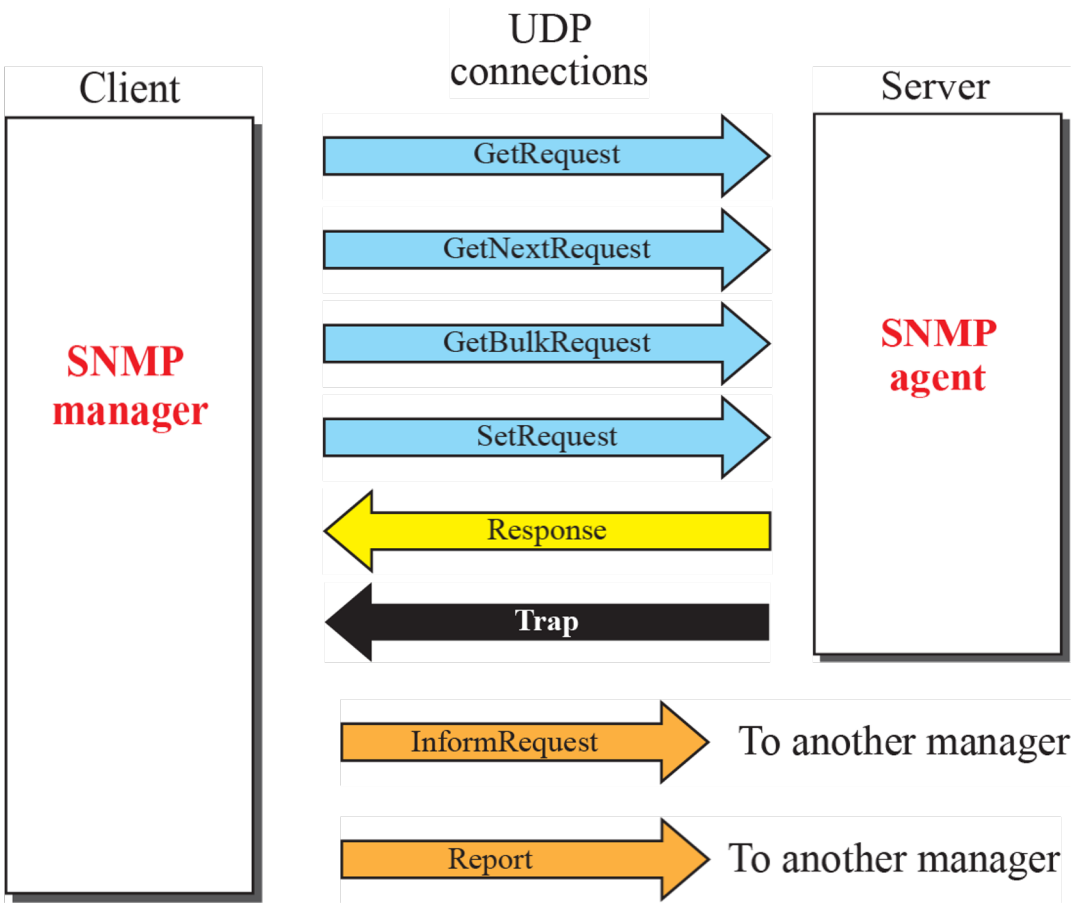
SNMP mechanism

- **SNMP manager**—Works on a network management system (NMS) to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and send traps to the NMS when some events, such as interface state change, occur.
- **Management Information Base (MIB)**—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.


Agent variables
Agent
Agent
Agent
Agent
Manager
Language syntax
Declaration and definition
Program coding
SMI
MIB
SNMP
Computer programming
Network management


Manager
Agent
Internet
Question
1
I want to know the number of UDP user datagrams received?
SMI
Integer values are defined using three attributes
MIB
The object has an integer value and is called udpInDatagram with id 1.3.6.1.2.1.7.1.0
SNMP
Encapsulate the request in a GetRequest message
2
3
SNMP packet
4
GetRequest
SNMP packet
Response
5
Answer
6
Six user datagram received.
Time
Time


1.3.6.1.2.1
mib-2
sys
if
at
ip
icmp
tcp
udp
egp
trans
snmp
1
2
3
4
5
6
7
8
10
11
udp
1.3.6.1.2.1.7
1
udpIn
Datagrams
2
udpNo
Ports
3
udpIn
Errors
4
udpOut
Datagrams
5
udpTable
1
udpEntry
1
udpLocal
Address
2
udpLocal
Port



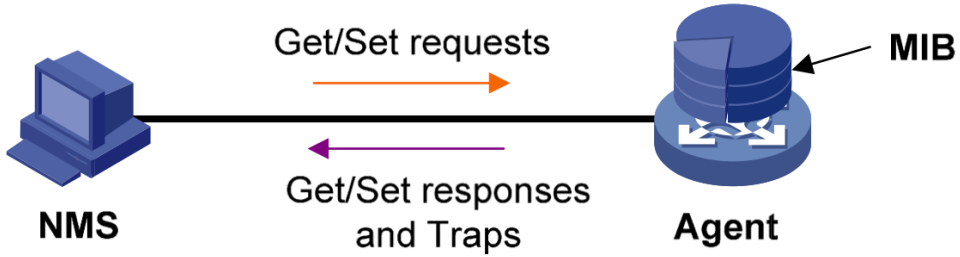
Type	*Tag (Hex)*	*Type*	*Tag (Hex)*
GetRequest	**A0**	GetBulkRequest	**A5**
GetNextRequest	**A1**	InformRequest	**A6**
Response	**A2**	Trap (SNMPv2)	**A7**
SetRequest	**A3**	Report	**A8**

a. Passive open by both client and server

b. Exchange of request and response messages

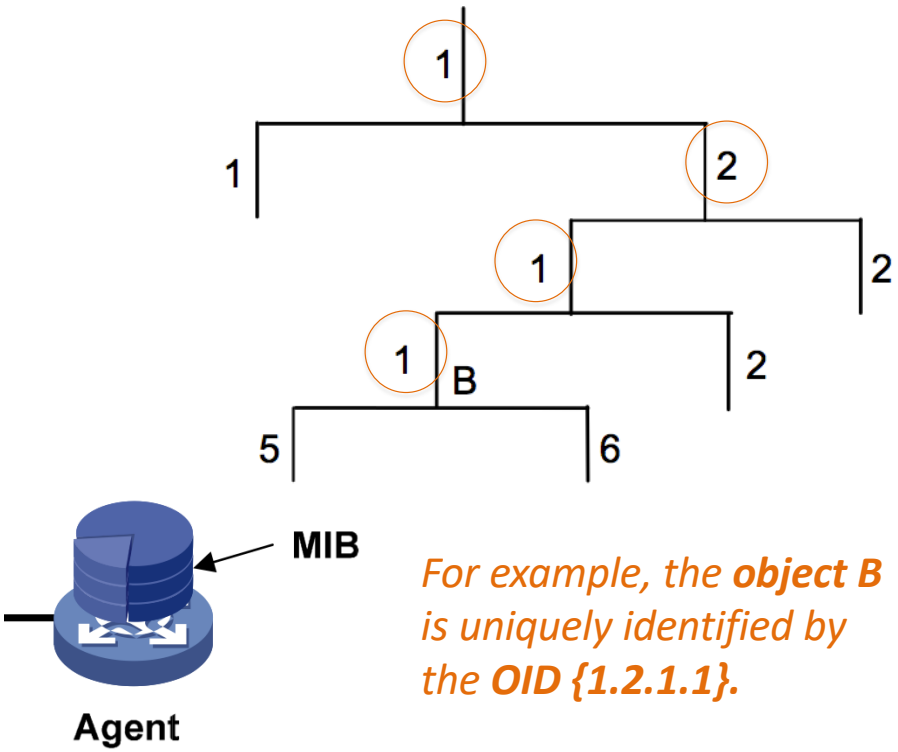
c. Server sends Trap message

Relationship between an NMS, agent and MIB



- **Get**—The NMS retrieves SNMP object nodes in an agent MIB.
- **Set**—The NMS modifies the value of an object node in the agent MIB.
- **Trap**—The SNMP agent sends traps to report events to the NMS.
- **Inform**—The NMS sends alarms to other NMSs.

Management Information Base



*For example, the **object B** is uniquely identified by the **OID {1.2.1.1}.***

- A MIB stores variables called ***nodes*** or ***objects*** in a tree hierarchy and identifies each node with a unique OID.
- An OID is a string of numbers that describes the path from the root node to a leaf node.

SNMP protocol versions

- **SNMPv1** : uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as set on the SNMP agent.
- **SNMPv2c** : also uses community names for authentication, but supports more operation modes, data types, and error codes.
- **SNMPv3** : uses a user-based security model (USM) to secure SNMP communication.

Table 1 SNMP Security Models and Levels

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 algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

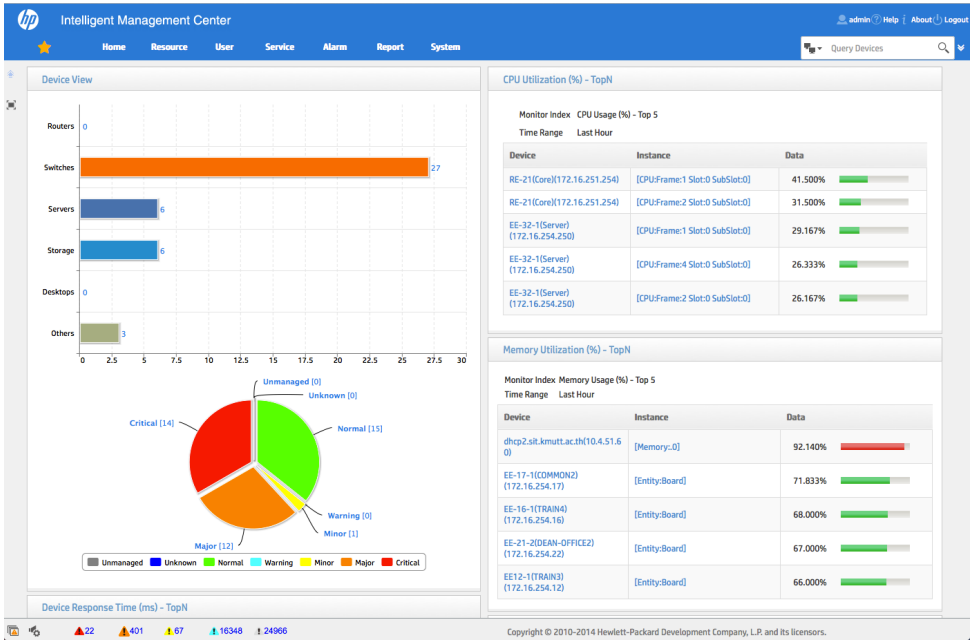
SNMPv3

- Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management.
- SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

SNMPv3

- **Message integrity**—Ensuring that a packet has not been tampered with in-transit.
- **Authentication**—Determining the message is from a valid source.
- **Encryption**—Scrambling the contents of a packet prevent it from being seen by an unauthorized source

HPE Intelligent Management Center (HPE IMC)



IMC management extends beyond HP

- Discovery & Topology
- Monitoring & Performance Management
- Data Center Orchestration
- Events & Traps
- Configuration Backup & Restore
  - Configuration comparison
  - Base-lining and change notification
- Bulk Configuration

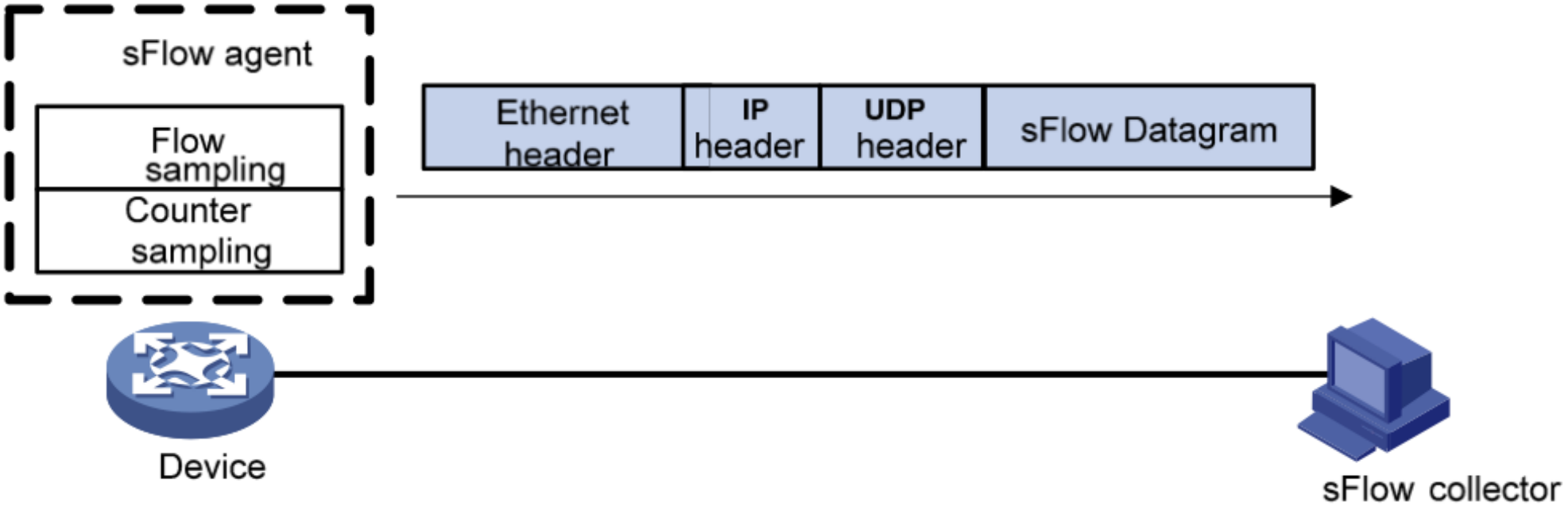
Single management solution for mixed HP & Cisco networks

- Simplifies Cisco / HP interworking & transitions
- Support for >2000 3rd party devices

sFlow

Sampled Flow

sFlow


sFlow agent
Flow sampling
Counter sampling
Ethernet header
IP header
UDP header
sFlow Datagram
Device
sFlow collector

Sampled Flow

- Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics.
- The sFlow agent collects traffic statistics and packet information from the sFlow-enabled interfaces and encapsulates them into sFlow packets. When the sFlow packet buffer is full, or the age time of sFlow packets is reached, the sFlow agent sends the packets to a specified sFlow collector.
- The sFlow collector analyzes the sFlow packets and displays the results.

Sampling mechanisms

- **Flow sampling**: Packet-based sampling, used to obtain packet content information.
- **Counter sampling**: Time-based sampling, used to obtain port traffic statistics.

NTP

Network Time Protocol

Network Time Protocol

- NTP overview Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients.
- NTP runs over the User Datagram Protocol (UDP), using UDP port 123.
- The purpose of using NTP is to keep consistent timekeeping among all clock-dependent devices within a network so that the devices can provide diverse applications based on the consistent time.

Clock strata

- **Stratum 0**

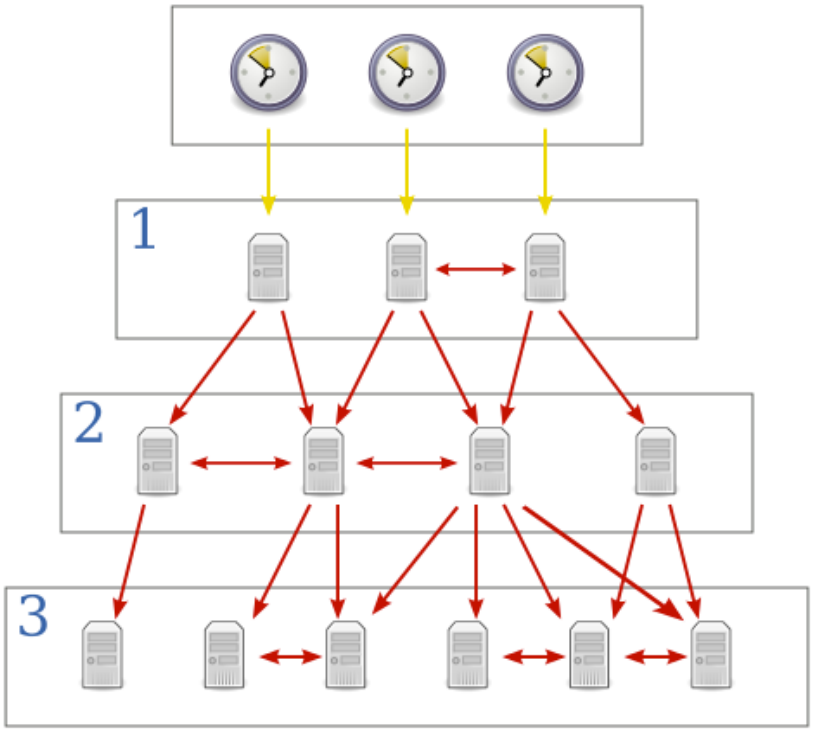
  These are high-precision timekeeping devices such as atomic (cesium, rubidium) clocks, GPS clocks or other radio clocks

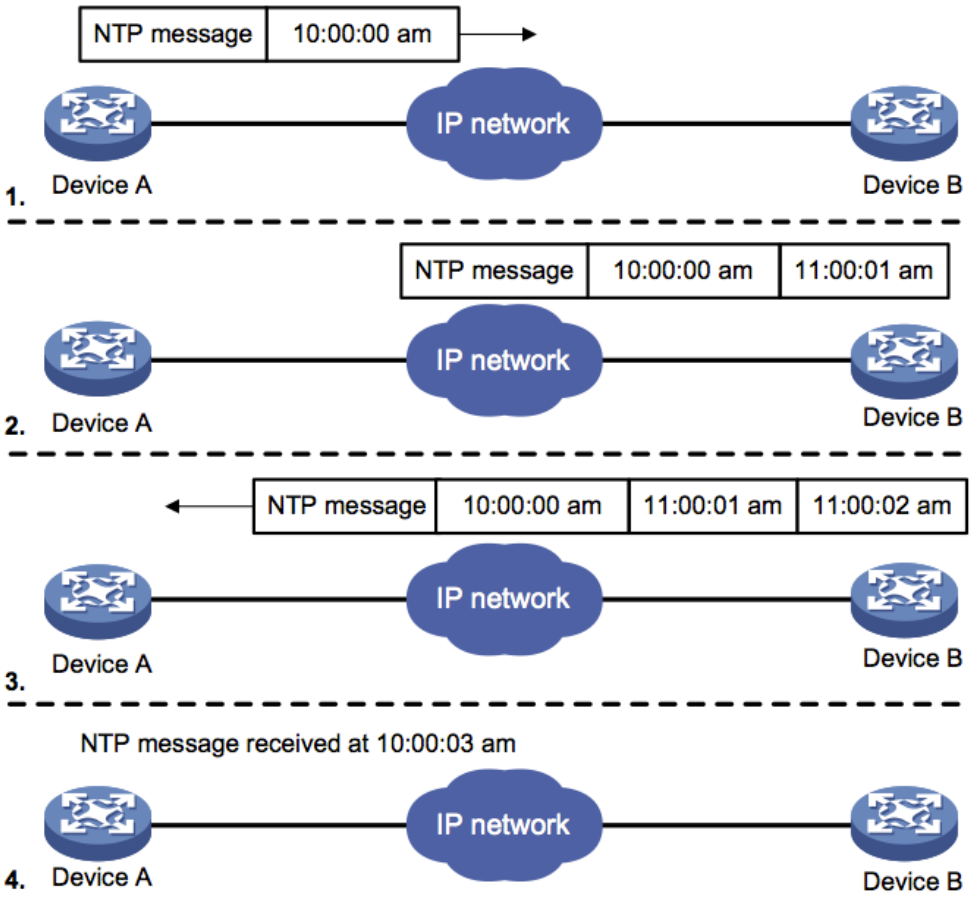
  Stratum 0 devices are also known as *reference clocks*.
- **Stratum 1**

  These are computers whose system clocks are synchronized to within a few microseconds of their attached stratum 0 devices. They are also referred to as primary time servers.
- **Stratum 2**

  These are computers that are synchronized over a network to stratum 1 servers. Often a stratum 2 computer will query several stratum 1 servers.
- **Stratum 3**

  They employ exactly the same algorithms for peering and data sampling as stratum 2, and can themselves act as servers for stratum 4 computers.





- Device A sends Device B an NTP message, which is timestamped when it leaves Device A. The time stamp is 10:00:00 am (T1).
- When this NTP message arrives at Device B, it is timestamped by Device B. The timestamp is 11:00:01 am (T2).
- When the NTP message leaves Device B, Device B timestamps it. The timestamp is 11:00:02 am (T3).10
- When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

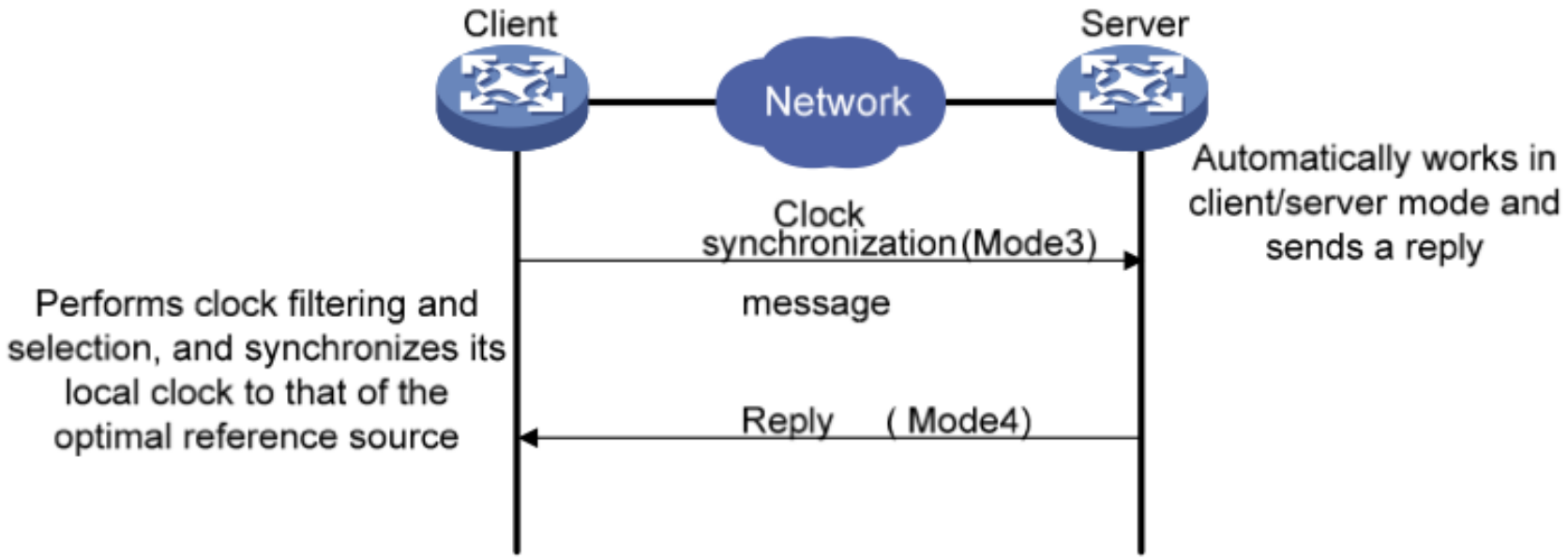
- The roundtrip delay of NTP message:

  Delay = (T4–T1) – (T3-T2) = 2 sec.

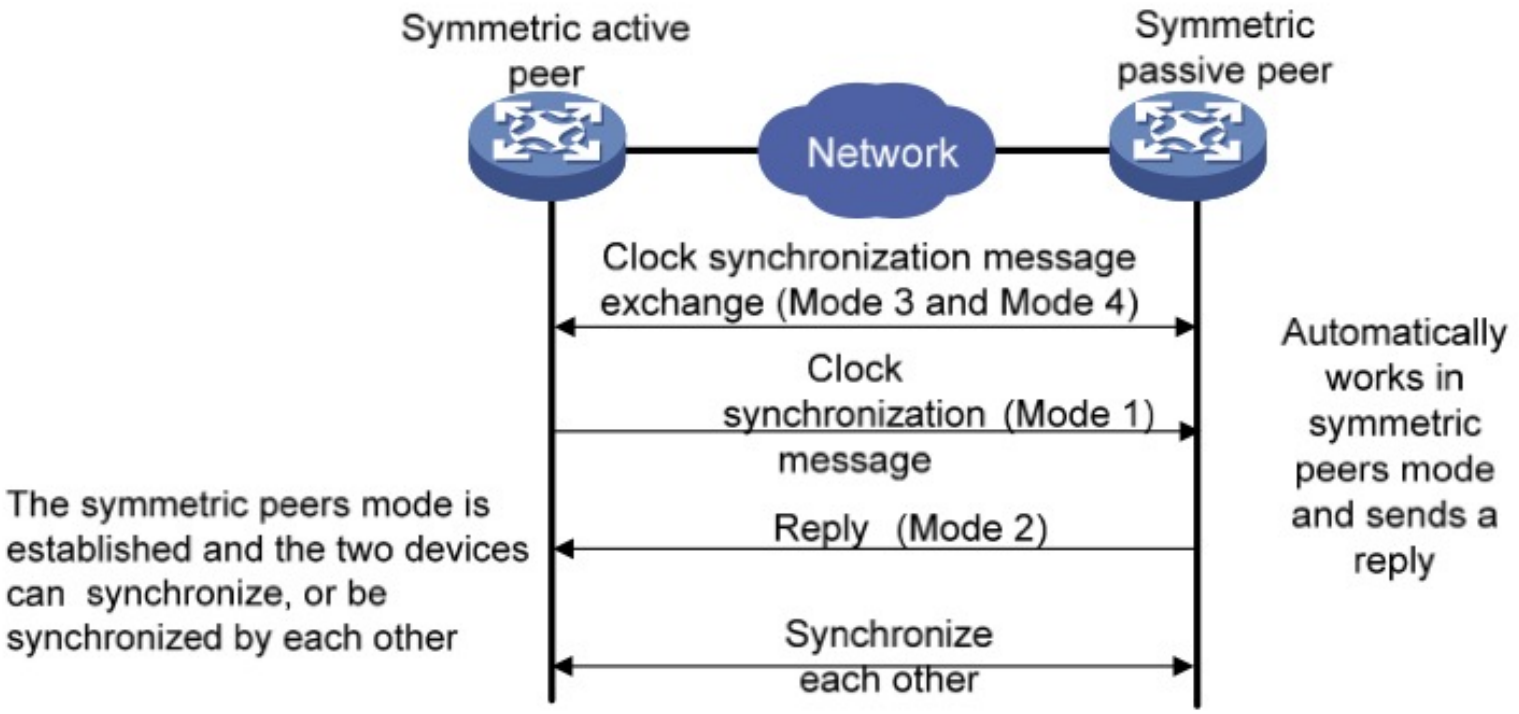
- Time difference between Device A and Device B:

  Offset = ((T2-T1) + (T3-T4))/2 = 1 hour.

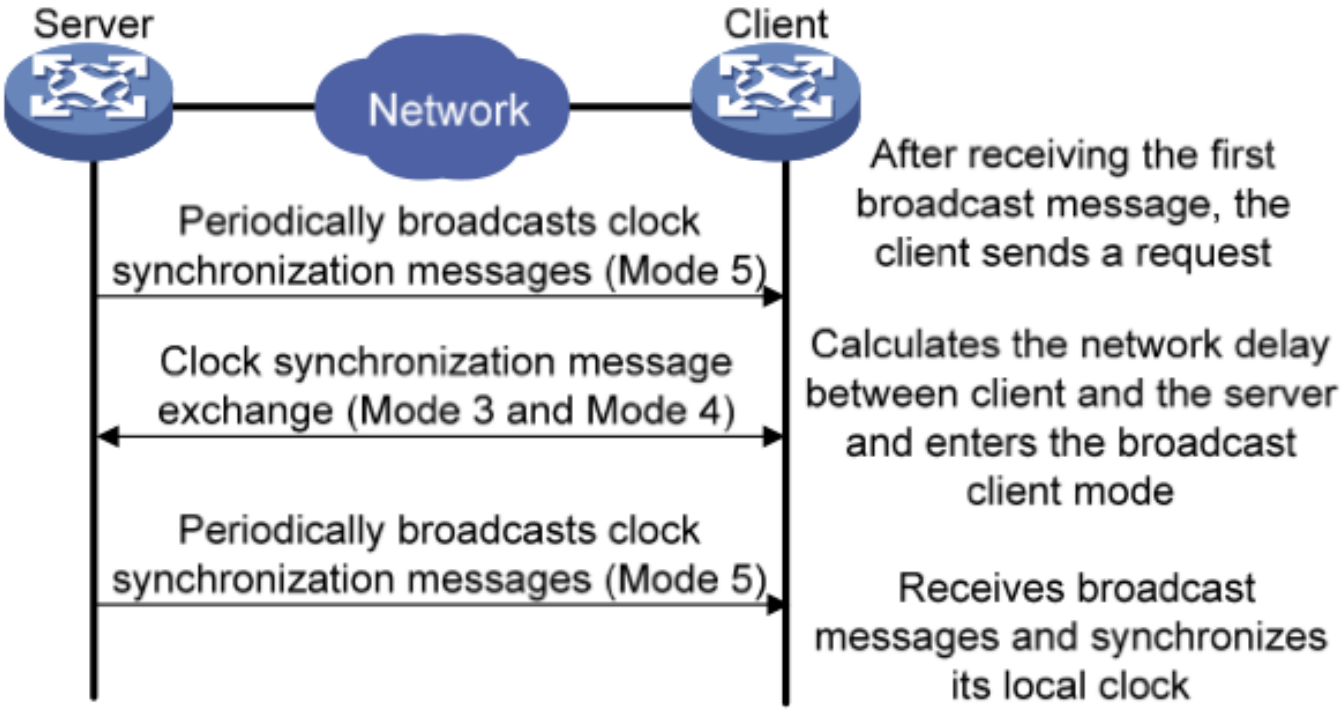
Client/server mode



Symmetric peer mode



Broadcast mode



Multicast mode