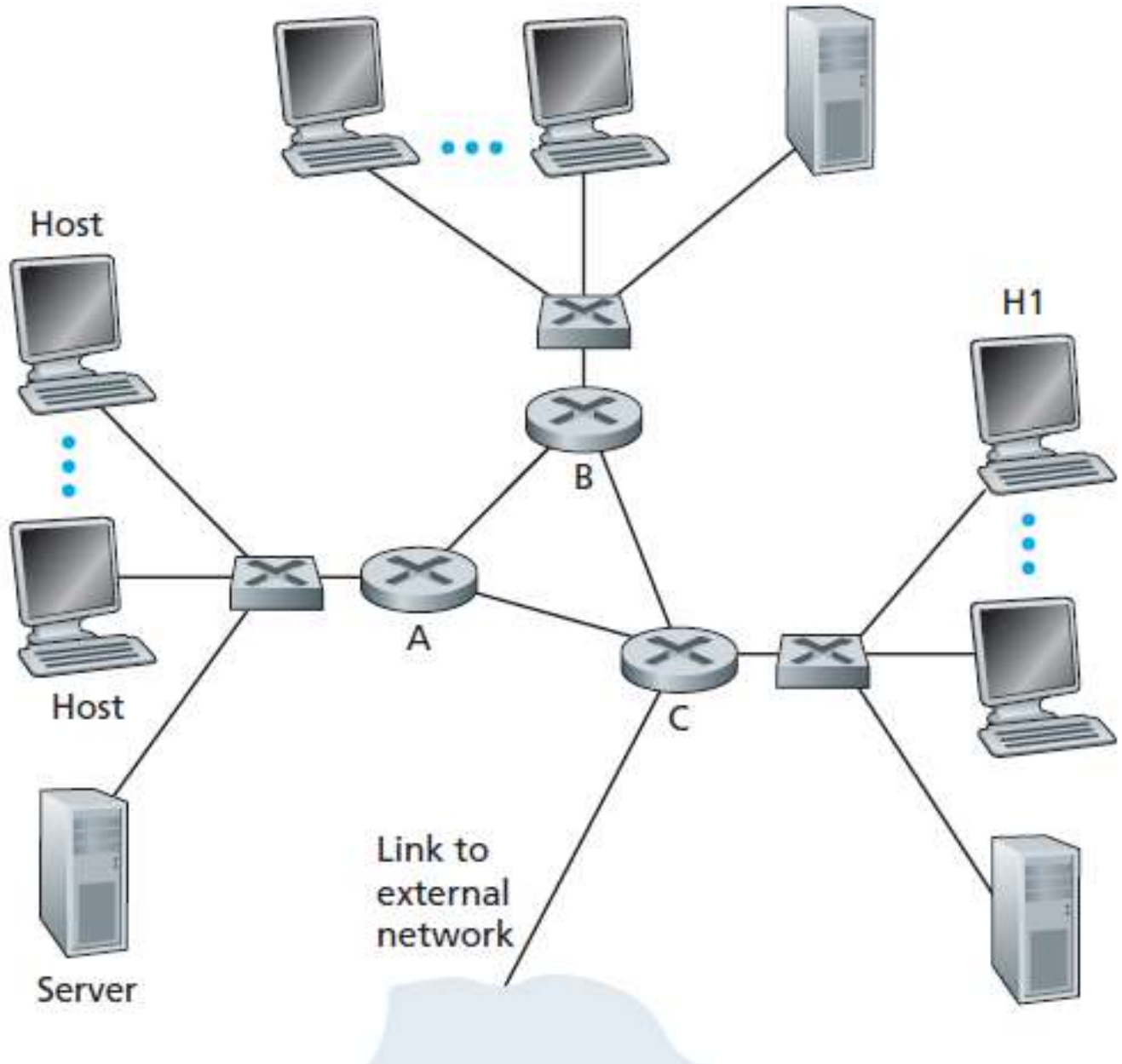
Introduction to network management

“What is network management?”

- *“Network management includes the deployment, integration, and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.”*

- The network administrator will actively monitor, manage, and control the system with which she or he is entrusted.
- As the public Internet and private intranets have grown from small networks into a large global infrastructure,
- the need to manage the huge number of hardware and software components within these networks more systematically has grown more important as well.


Host
Host
Server
A
B
C
H1
Link to
external
network

- Figure illustrates a small network consisting of three routers and a number of hosts and servers.
- Even in such a simple network, there are many scenarios in which a network administrator might benefit tremendously from having appropriate network management tools:
- *Detecting failure of an interface card at a host or a router.*
- With appropriate network management tools, a network entity (for example, router A) may report to the network administrator that one of its interfaces has gone down.
- if the administrator noted an increase in checksum errors in frames being sent by the soon-to-die interface.

- *Host monitoring.* Here, the network administrator might periodically check to see if all network hosts are up and operational. The network administrator may really be able to impress a network user by proactively responding to a problem (host down) before it is reported by a user.
- *Monitoring traffic to aid in resource deployment.* A network administrator might monitor source-to-destination traffic patterns and notice, for example, that by switching servers between LAN segments, the amount of traffic that crosses multiple LANs could be significantly decreased.
- when better performance is achieved with no new equipment costs.
- Similarly, by monitoring link utilization, a network administrator might determine that a LAN segment or the external link to the outside world is overloaded.

- *Detecting rapid changes in routing tables.*
- Route flapping—frequent changes in the routing tables—may indicate instabilities in the routing or a misconfigured router.
- Certainly, the network administrator who has improperly configured a router would prefer to discover the error him- or herself, before the network goes down.
- *Monitoring for SLAs*. **Service Level Agreements (SLAs)** are contracts that define specific performance metrics and acceptable levels of network-provider performance with respect to these metrics .
- These SLAs include service availability (outage), latency, throughput, and outage notification requirements.
- Clearly, if performance criteria are to be part of a service agreement between a network provider and its users, then measuring and managing performance will be of great importance to the network administrator.

- *Intrusion detection.* A network administrator may want to be notified when network traffic arrives from, or is destined for, a suspicious source (for example, host or port number).
- Similarly, a network administrator may want to detect (and in many cases filter) the existence of certain types of traffic (for example, sourcerouted packets, or a large number of SYN packets directed to a given host) that are known to be characteristic of the types of security attacks.

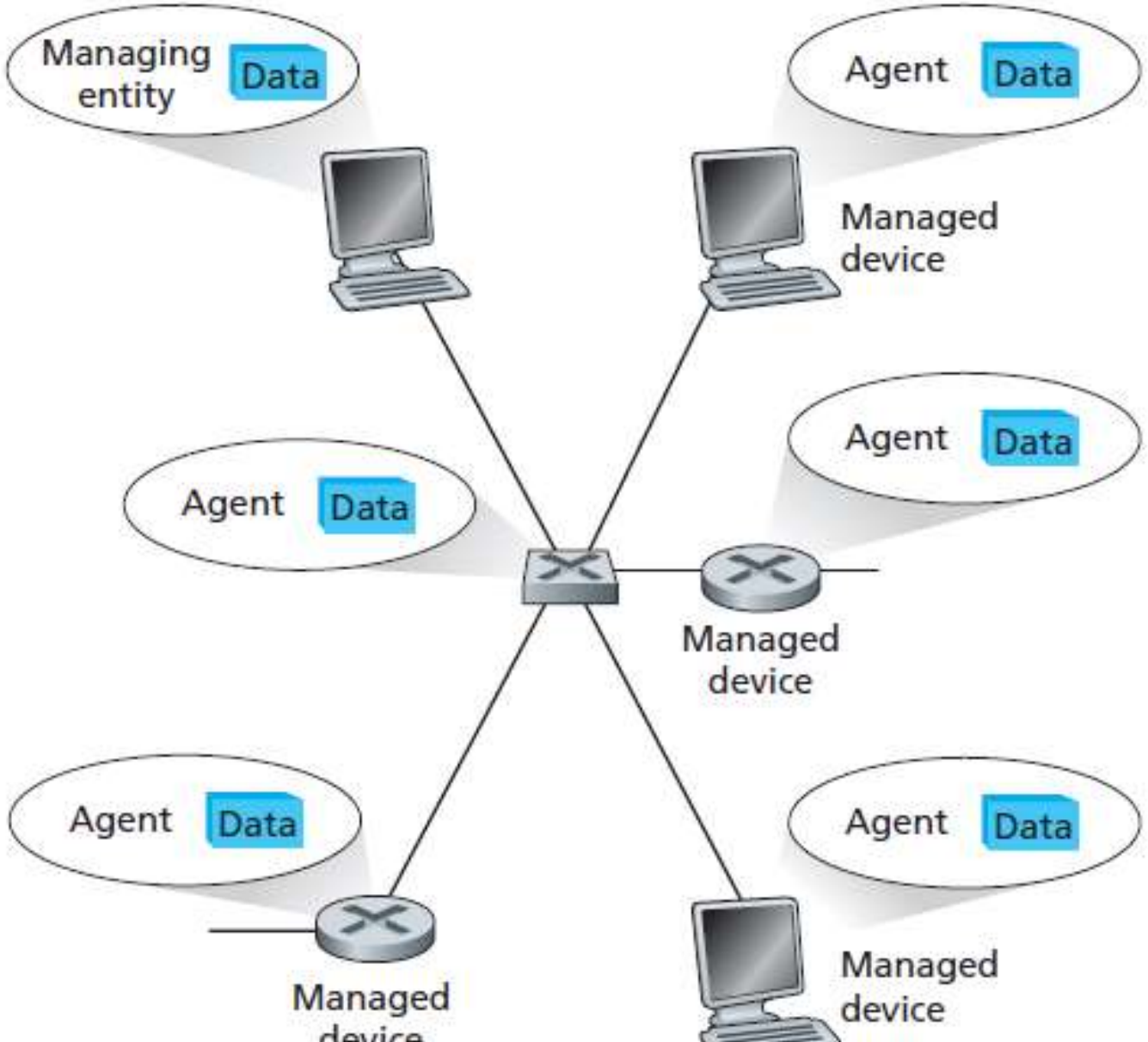
Five areas of network management

- *Performance management.* The goal of performance management is to quantify, measure, report, analyze, and control the performance (for example, utilization and throughput) of different network components.
- These components include individual devices (for example, links, routers, and hosts) as well as end-to-end abstractions such as a path through the network.
- Simple Network Management Protocol (SNMP) play a central role in Internet performance management.

- *Fault management*. The goal of fault management is to log, detect, and respond to fault conditions in the network.
- The line between fault management and performance management is rather blurred.
- We can think of fault management as the immediate handling of transient network failures (for example, link, host, or router hardware or software outages), while performance management takes the longer-term view of providing acceptable levels of performance in the face of varying traffic demands and occasional network device failures.

- *Configuration management.* Configuration management allows a network manager to track which devices are on the managed network and the hardware and software configurations of these devices.
- *Accounting management.* Accounting management allows the network manager to specify, log, and control user and device access to network resources.
- Usage quotas, usage-based charging, and the allocation of resource-access privileges all fall under accounting management.
- *Security management.* The goal of security management is to control access to network resources according to some well-defined policy.
- The use of firewalls to monitor and control external access points to one's network.

The Infrastructure for Network Management



- There are three principal components of a network management architecture:
- a managing entity
- the managed devices
- and a network management protocol.

- The **managing entity** is an application, typically with a human in the loop, running in a centralized network management .
- The managing entity is the locus of activity for network management; it controls the collection, processing, analysis, and/or display of network management information.
- It is here that actions are initiated to control network behavior and here that the human network administrator interacts with the network devices.

- A **managed device** is a piece of network equipment (including its software) that resides on a managed network. This is the branch office in our human analogy.
- A managed device might be a host, router, bridge, hub, printer, or modem.
- Within a managed device, there may be several so-called **managed objects**. These managed objects are the actual pieces of hardware within the managed device (for example, a network interface card), and the sets of configuration parameters for the pieces of hardware and software (for example, an intradomain routing protocol such as RIP).
- These managed objects have pieces of information associated with them that are collected into a **Management Information Base.**
- Finally, also resident in each managed device is a **network management agent**, a process running in the managed device that communicates with the managing entity, taking local actions at the managed device under the command and control of the managing entity.

- The third piece of a network management architecture is the **network management protocol**.
- The protocol runs between the managing entity and the managed devices, allowing the managing entity to query the status of managed devices and indirectly take actions at these devices via its agents.
- Agents can use the network management protocol to inform the managing entity of exceptional events (for example, component failures or violation of performance thresholds).
- It’s important to note that the network management protocol does not itself manage the network.
- Instead, it provides capabilities that a network administrator can use to manage (“monitor, test, poll, configure, analyze, evaluate, and control”) the network.