Lecture 21 – Intrusion Detection

November 6, 2018

Dr. Dan Massey

Motivating Example: SNORT Rule

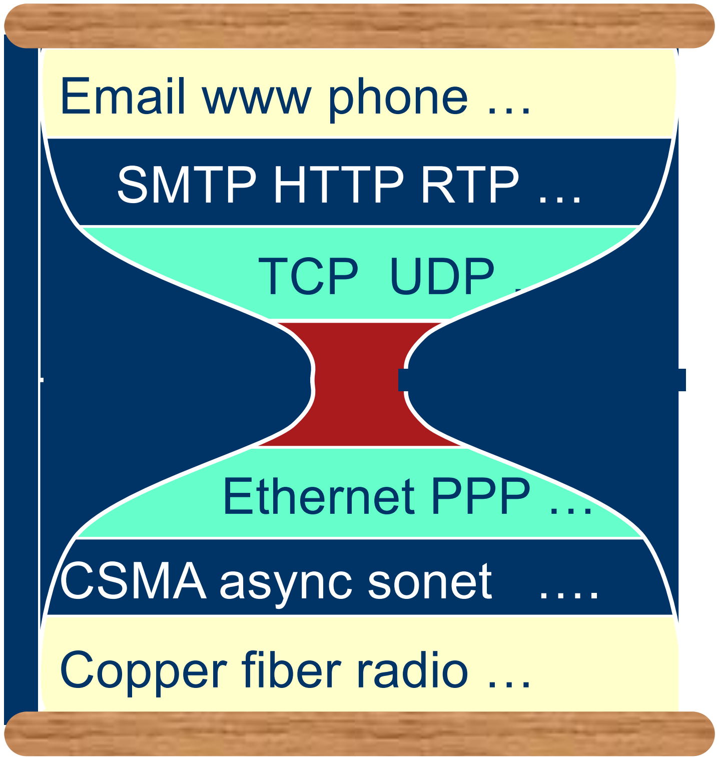
- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps command attempt"; flow:to_server,established; uricontent:"/bin/ps"; nocase; classtype:web-application-attack; sid:1328; rev:6;)

Network Layer Basics: IP Format and Addressing
Transport Layer Basics: UDP/TCP Header and connections
Application Layer: vast numbers of applications

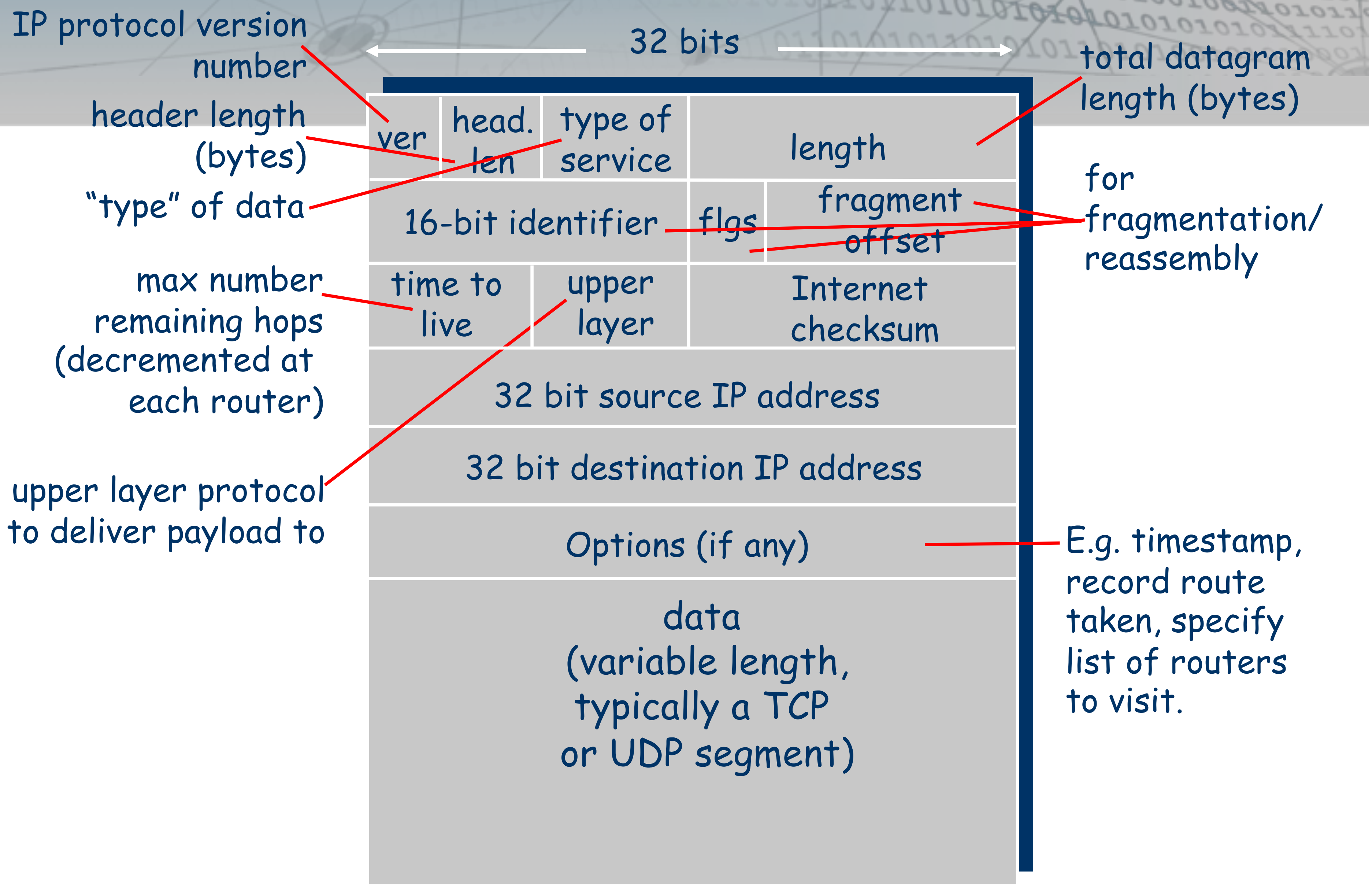
Establish a Set of Basic Network Concepts

Internet is a Layered Architecture

- Application layer
  - Communication between networked applications
  - Protocols: HTTP, FTP, NTP, and many others
- Transport layer
  - Communication between processes
  - Protocols: TCP and UDP
- Network layer
  - Communication between nodes
  - Protocols: IP
- Link and Physical Layers
  - Communication between devices
  - Ethernet, WifI, Bluetooth, and many others



IP Datagram Format



IP protocol version number

header length (bytes)

"type" of data

max number remaining hops (decremented at each router)

upper layer protocol to deliver payload to

32 bits

ver

head. len

type of service

length

16-bit identifier

flgs

fragment offset

time to live

upper layer

Internet checksum

32 bit source IP address

32 bit destination IP address

Options (if any)

data (variable length, typically a TCP or UDP segment)

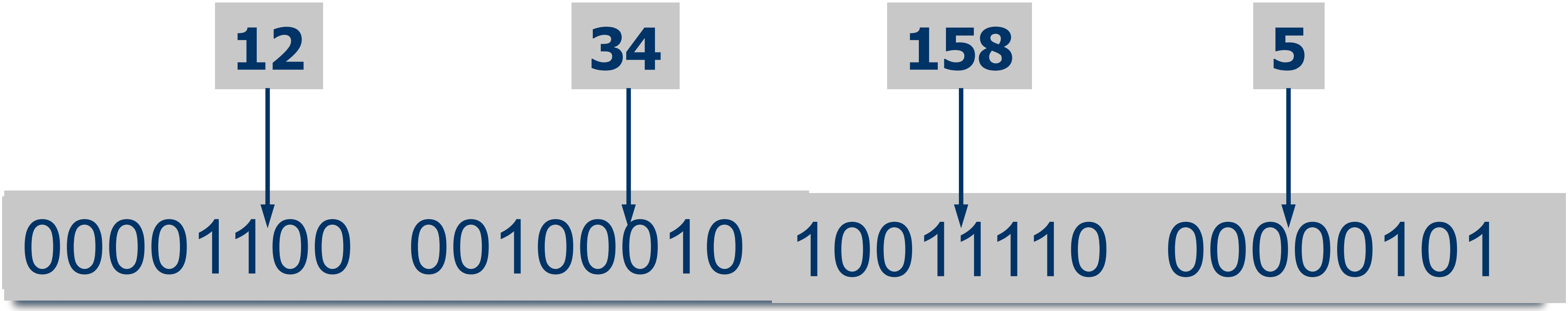
total datagram length (bytes)

for fragmentation/ reassembly

E.g. timestamp, record route taken, specify list of routers to visit.

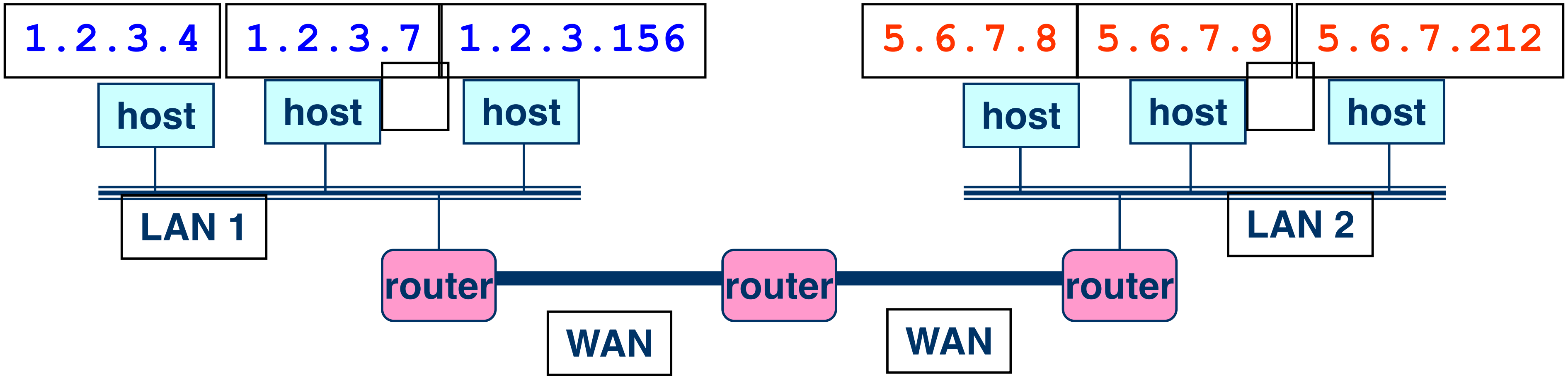
IP Address (IPv4)

- A unique 32-bit number
  (i.e., 4B addresses)
- Identifies an interface
  (on a host, on a router, …)
- Represented in dotted-quad notation



IP Addressing and Subnets

- Number related hosts from a common subnet
  - 1.2.3.0/24 on the left LAN
  - 5.6.7.0/24 on the right LAN

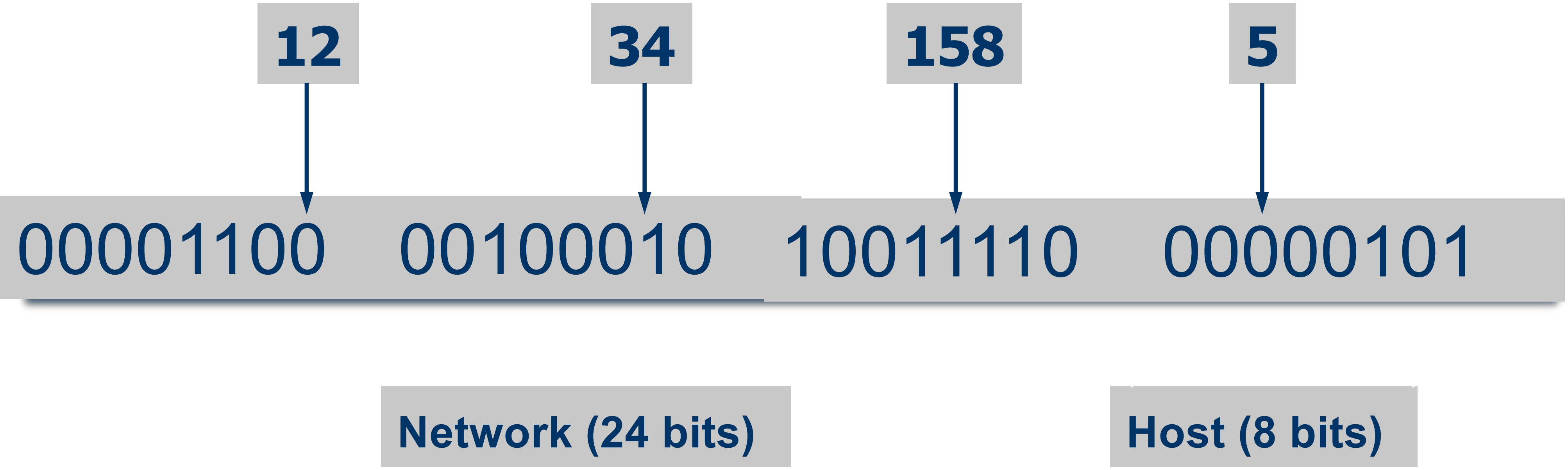


1.2.3.0/24	←
5.6.7.0/24	→

forwarding table

Hierarchical Addressing: IP Prefixes

- Divided into network & host portions (left and right)
- 12.34.158.0/24 is a 24-bit prefix with 2^8 addresses



12 34 158 5

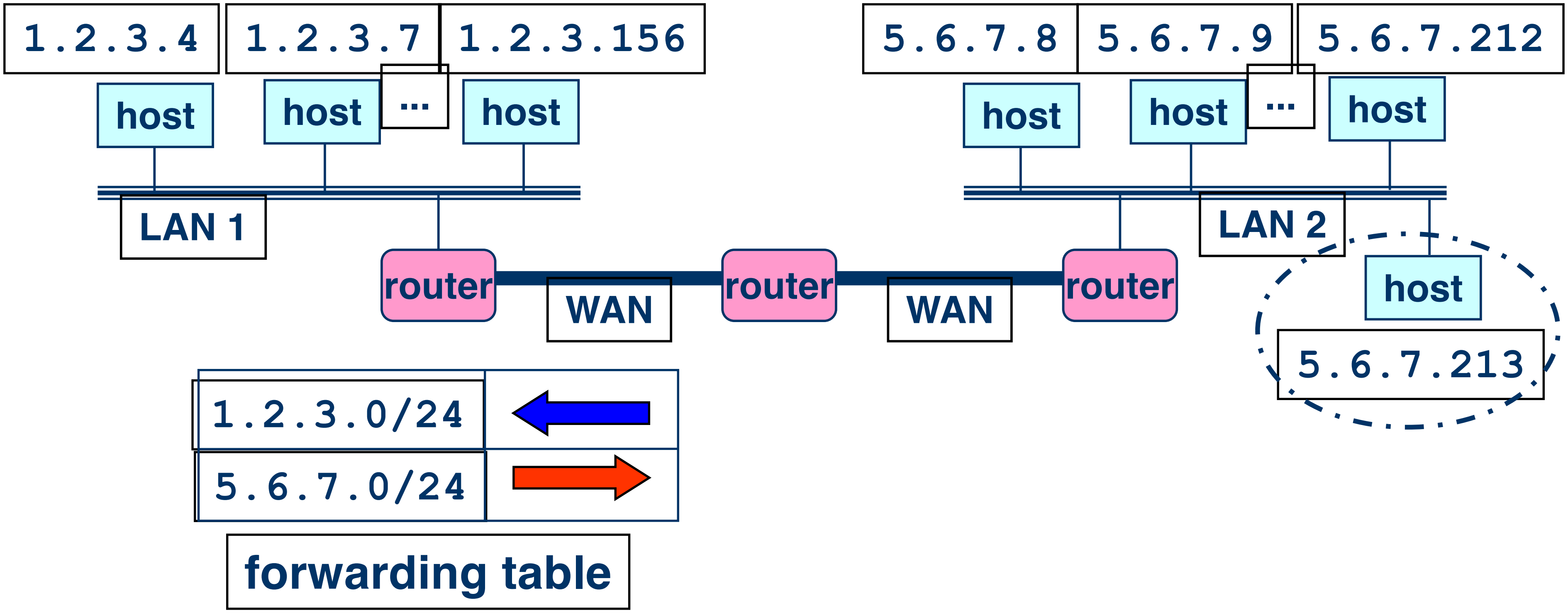
00001100 00100010 10011110 00000101

Network (24 bits)

Host (8 bits)

Easy to Add New Hosts

- No need to update the routers
  - E.g., adding a new host 5.6.7.213 on the right
  - Doesn't require adding a new forwarding entry

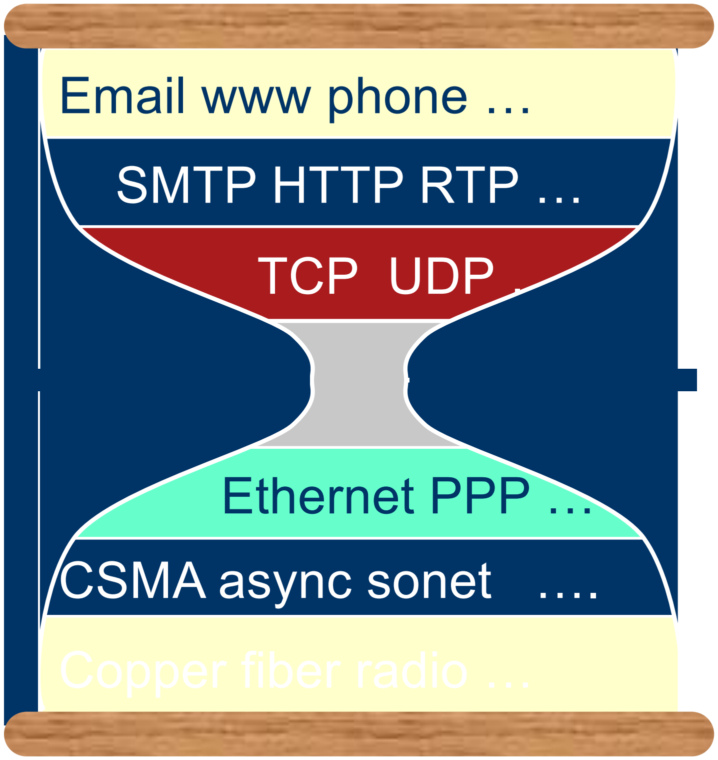


1.2.3.0/24	←
5.6.7.0/24	→

forwarding table

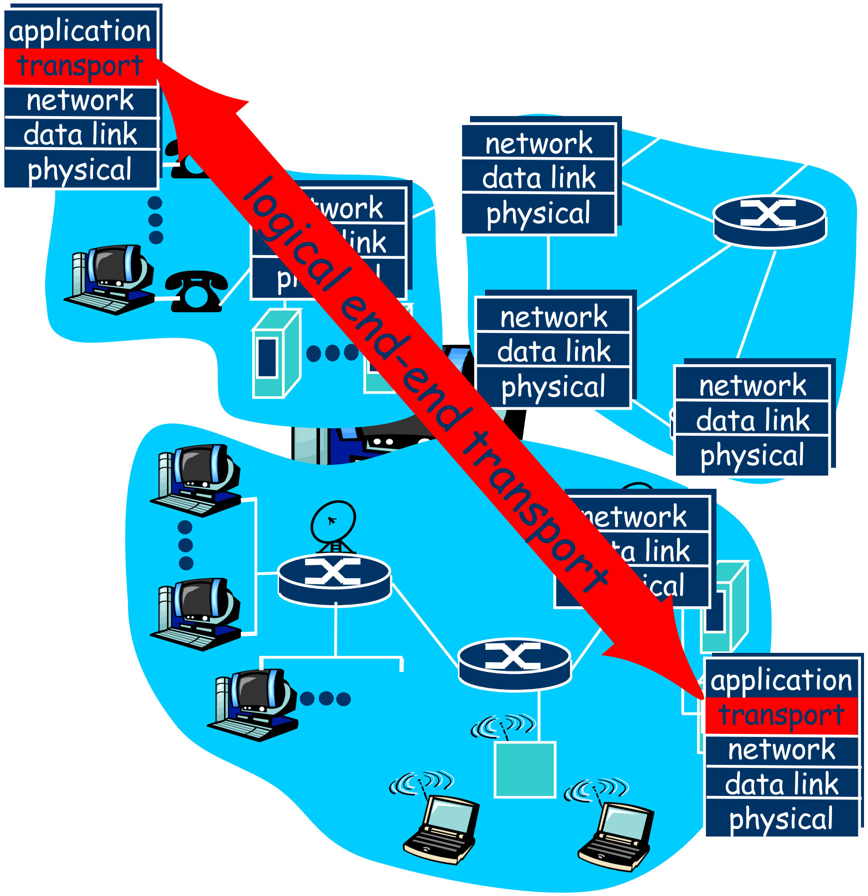
Role of Transport Layer

- Application layer
  - Communication between networked applications
  - Protocols: HTTP, FTP, NNTP, and many others
- **Transport layer**
  - **Communication between processes**
  - **Relies on network layer and serves the application layer**
  - **Protocols: TCP and UDP**
- Network layer
  - Communication between nodes
  - Protocols: IP



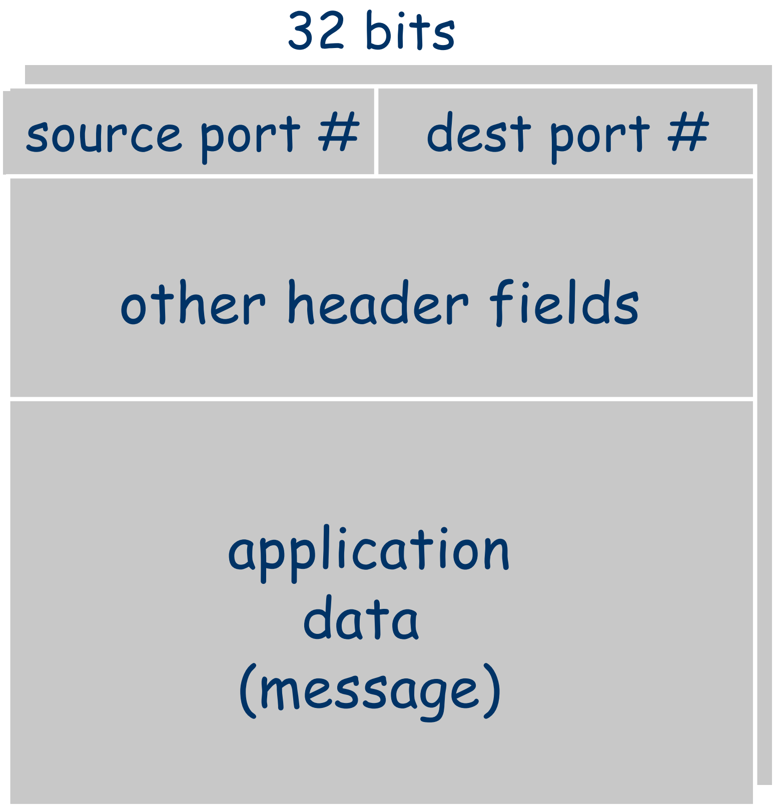
Transport Protocols

- Provide *logical communication* between application processes running on different hosts
- Run on end hosts
  - Sender: breaks application messages into segments, and passes to network layer
  - Receiver: reassembles segments into messages, passes to application layer
- Multiple transport protocol available to applications
  - Internet: TCP and UDP



Multiplexing and Demultiplexing

- Host receives IP datagrams
  - Each datagram has source and destination IP address,
  - Each datagram carries one transport-layer segment
  - Each segment has source and destination port number
- Host uses IP addresses and port numbers to direct the segment to appropriate socket



32 bits

source port #

dest port #

other header fields

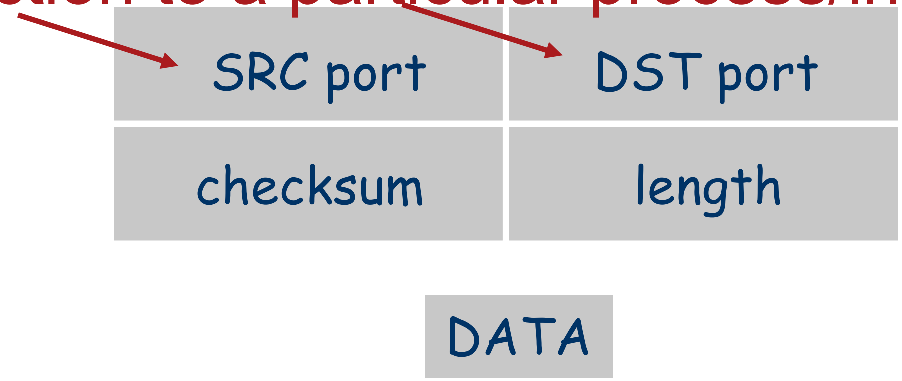
application data (message)

TCP/UDP segment format

User Datagram Protocol (UDP)

- Lightweight communication between processes
  - Avoid overhead and delays of ordered, reliable delivery
  - Send messages to and receive them from a socket
- Lightweight delivery service
  - IP plus port numbers to support (de)multiplexing
  - Optional error checking on the packet contents

Ties the connection to a particular process/instance



SRC port

DST port

checksum

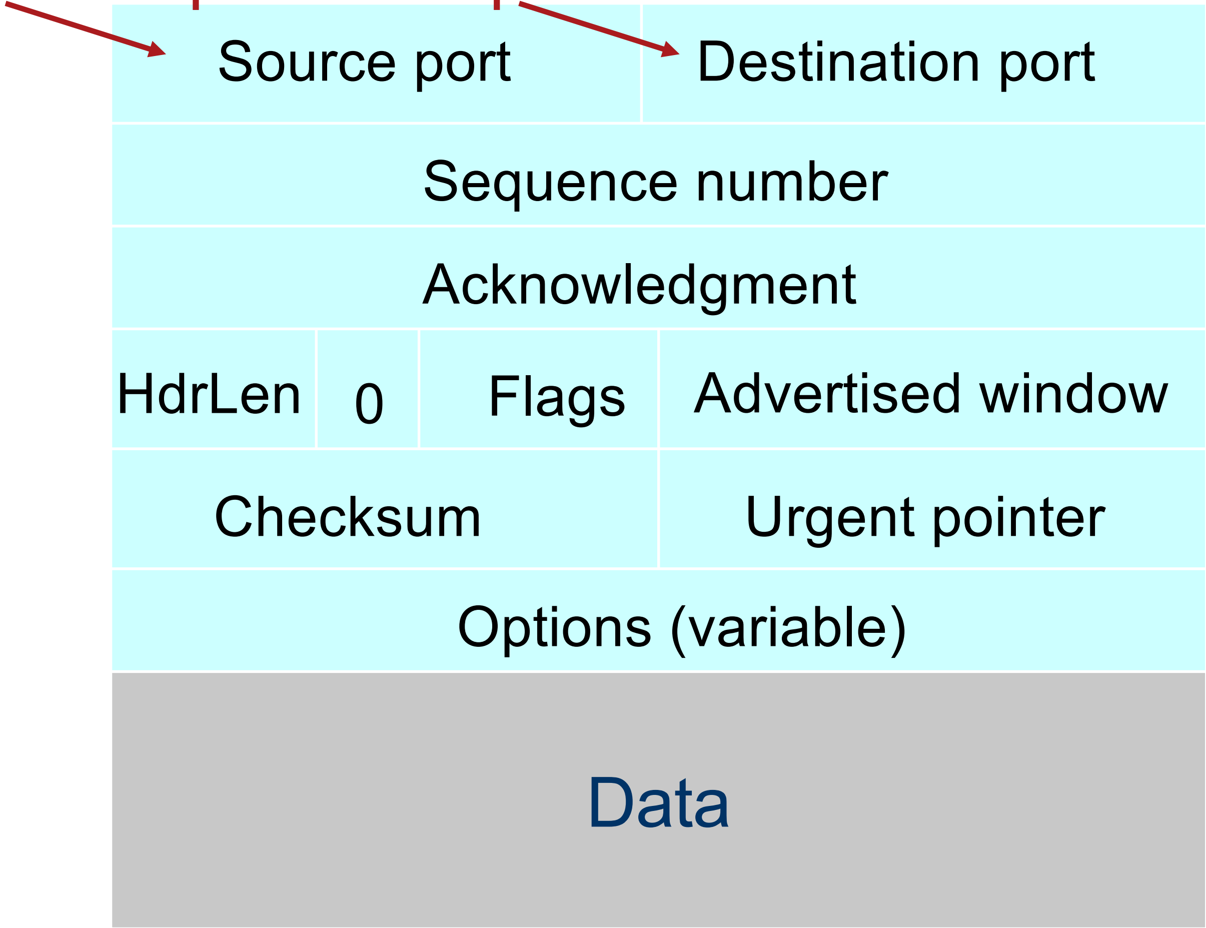
length

DATA

Ex: port 53 typically indicates DNS

TCP Header

Ties the connection to a particular process/instance



Source port

Destination port

Sequence number

Acknowledgment

HdrLen

0

Flags

Advertised window

Checksum

Urgent pointer

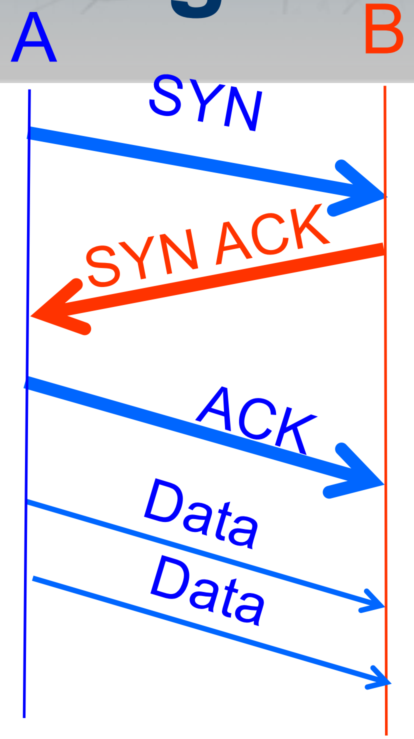
Options (variable)

Data

Flags: SYN
FIN
RST
PSH
URG
ACK

Ex: port 80 typically indicates web/http

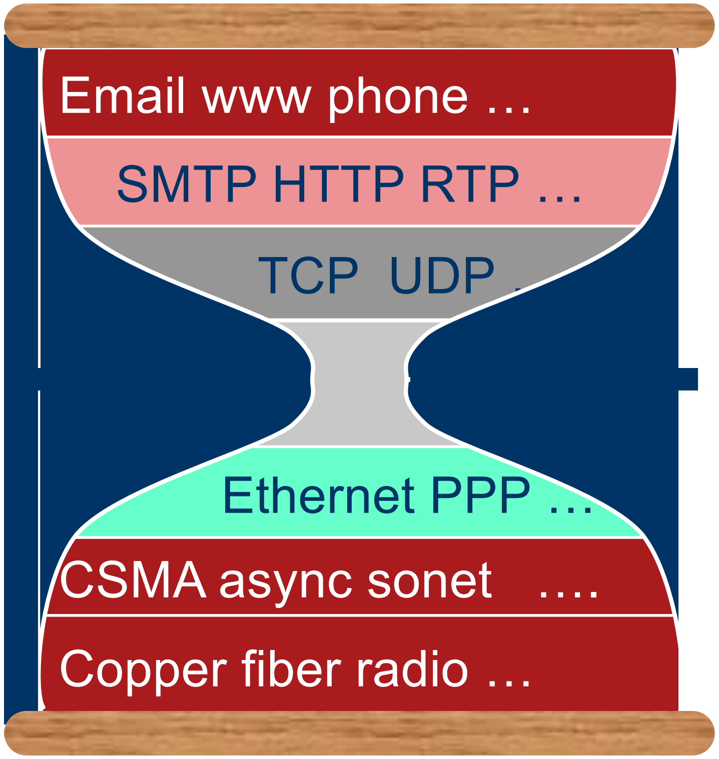
Establishing a TCP Connection



- Three-way handshake to establish connection
  - Host A sends a **SYN** (open) to the host B
  - Host B returns a SYN acknowledgment (**SYN ACK**)
  - Host A sends an **ACK** to acknowledge the SYN ACK

Link, Physical, and Application Layers

- Typically not the focus of general cybersecurity
- Application layer
  - Many standardized protocols (IETF and others)
  - Protocols may be proprietary
- Link and Physical Layers
  - Changes as packet traverses Internet
  - Protocols depend on locations
- Domain experts at the application and link/physical layers can (and do) use these features in cybersecurity.
  - We will focus on Transport and Network Layers



Motivating Example: SNORT Rule

- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ps command attempt"; flow:to_server,established; uricontent:"/bin/ps"; nocase; classtype:web-application-attack; sid:1328; rev:6;)

Network Layer Basics: IP Format and Addressing
Transport Layer Basics: UDP/TCP Header and connections
Application Layer: vast numbers of applications

Read Computer Security: Principle and Practices Chapter 8

Intrusion Detection

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intruder Behavior

Target acquisition and information gathering

Initial access

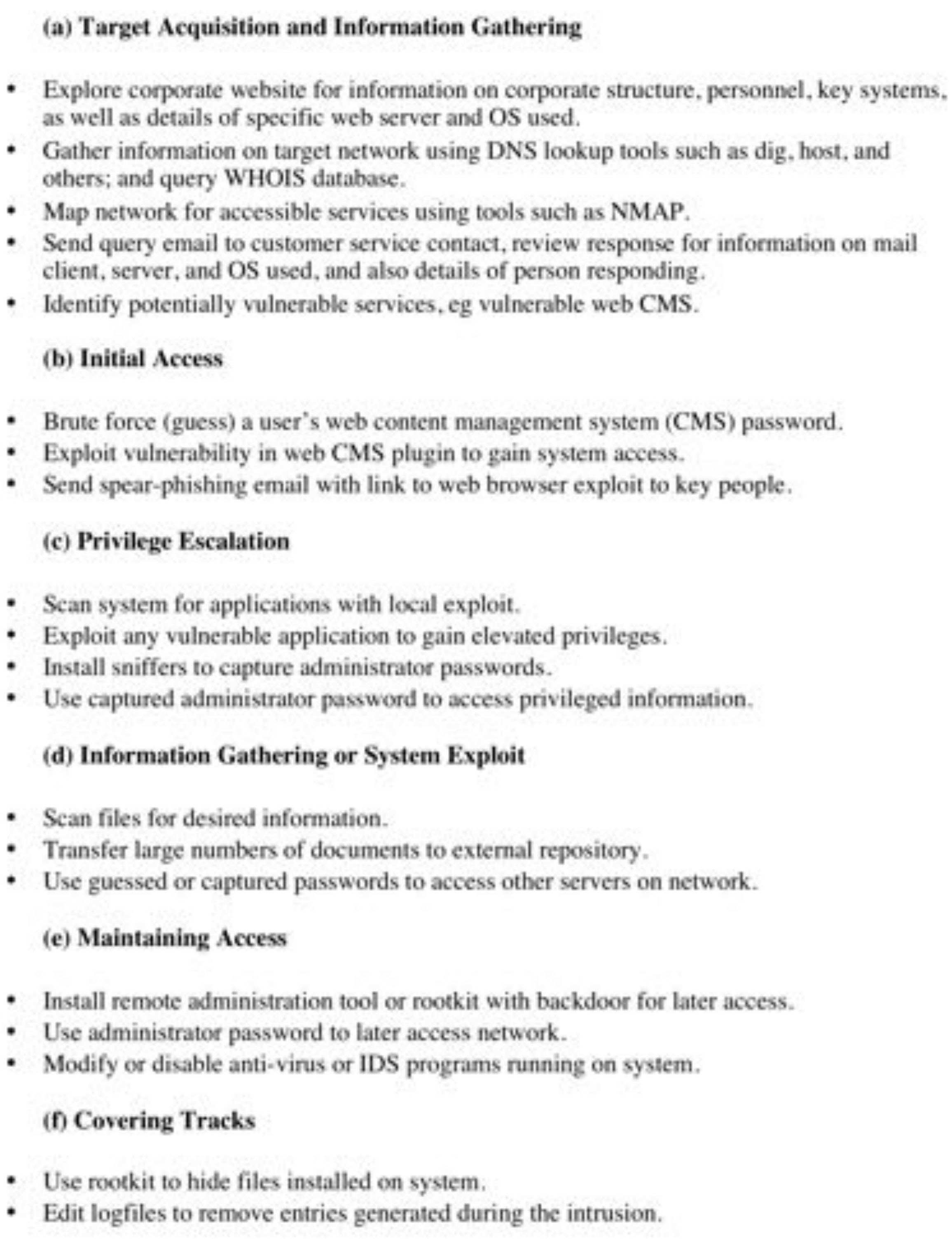
Privilege escalation

Information gathering or system exploit

Maintaining access

Covering tracks

Examples of Intruder Behavior



(a) Target Acquisition and Information Gathering

- Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
- Map network for accessible services using tools such as NMAP.
- Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, eg vulnerable web CMS.

(b) Initial Access

- Brute force (guess) a user's web content management system (CMS) password.
- Exploit vulnerability in web CMS plugin to gain system access.
- Send spear-phishing email with link to web browser exploit to key people.

(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Definitions

- Security Intrusion:

  Unauthorized act of bypassing the security mechanisms of a system

- Intrusion Detection:

  A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions

Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
  - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

Comprises three logical components:

- **Sensors - collect data**
- **Analyzers - determine if intrusion has occurred**
- **User interface - view output or control system behavior**

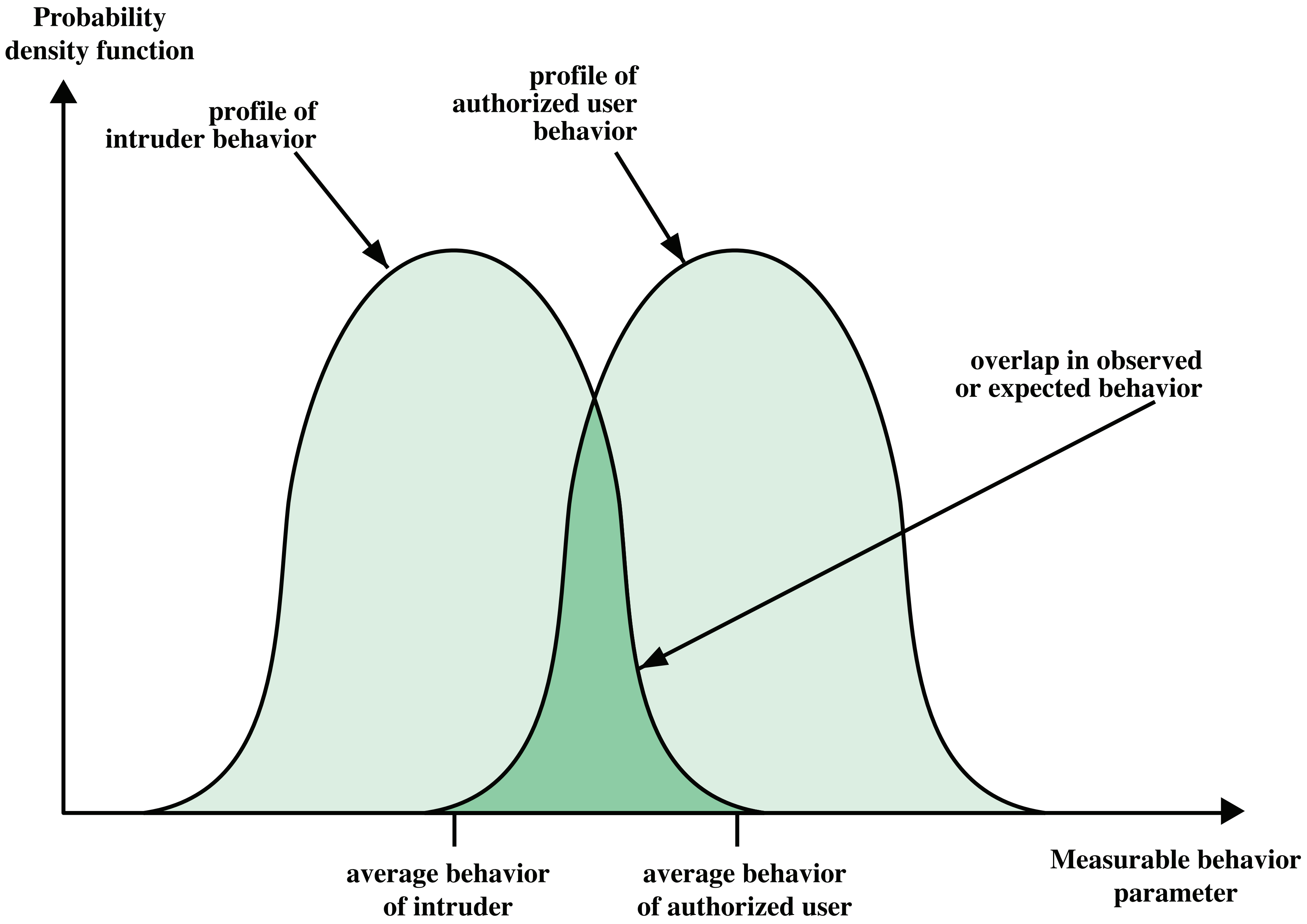


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

A variety of classification approaches are used:

Statistical

- Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics

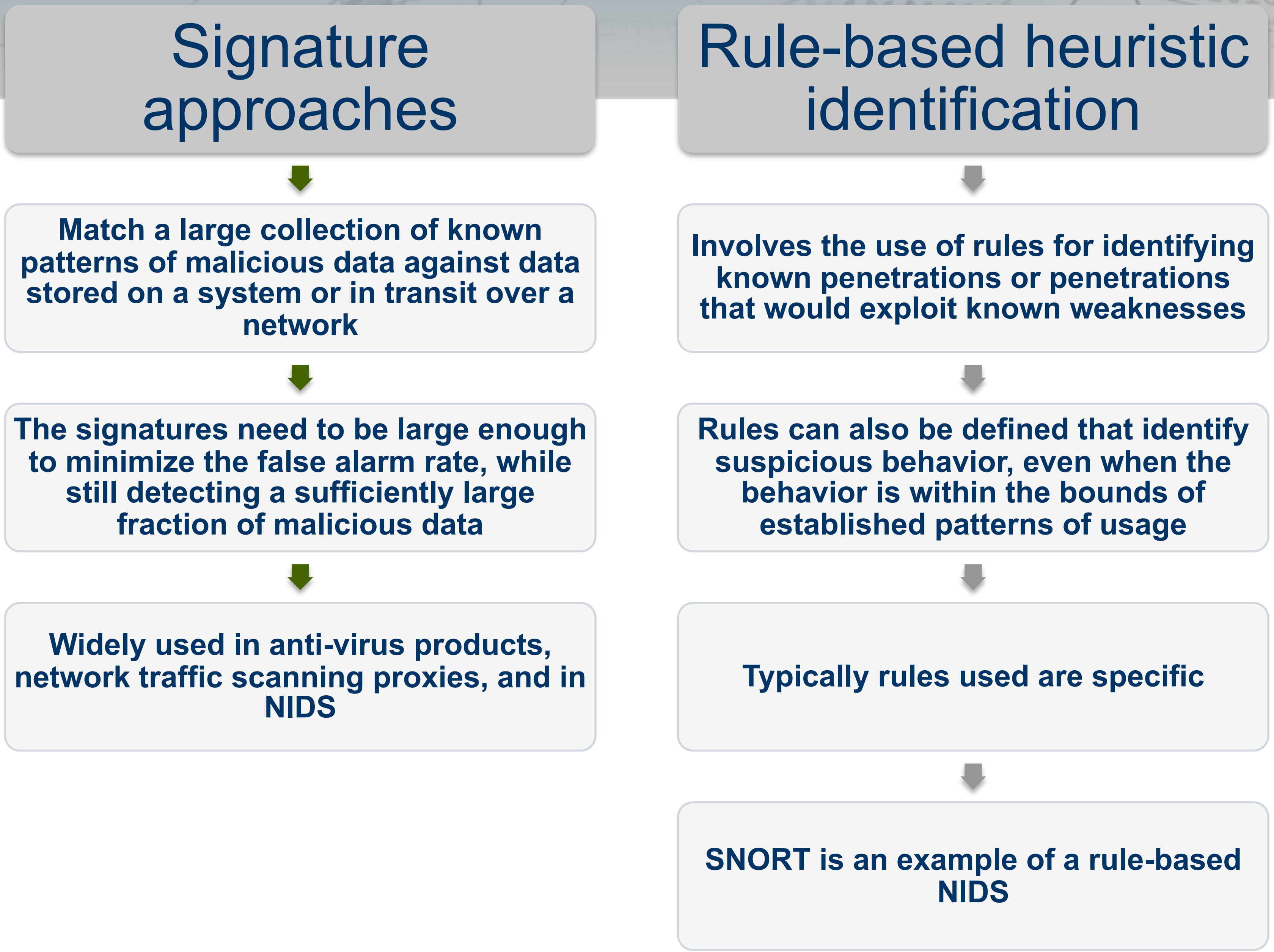
Knowledge based

- Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior

Machine-learning

- Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection



Signature approaches

Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

Data Sources and Sensors

A fundamental component of intrusion detection is the sensor that collects data

Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access

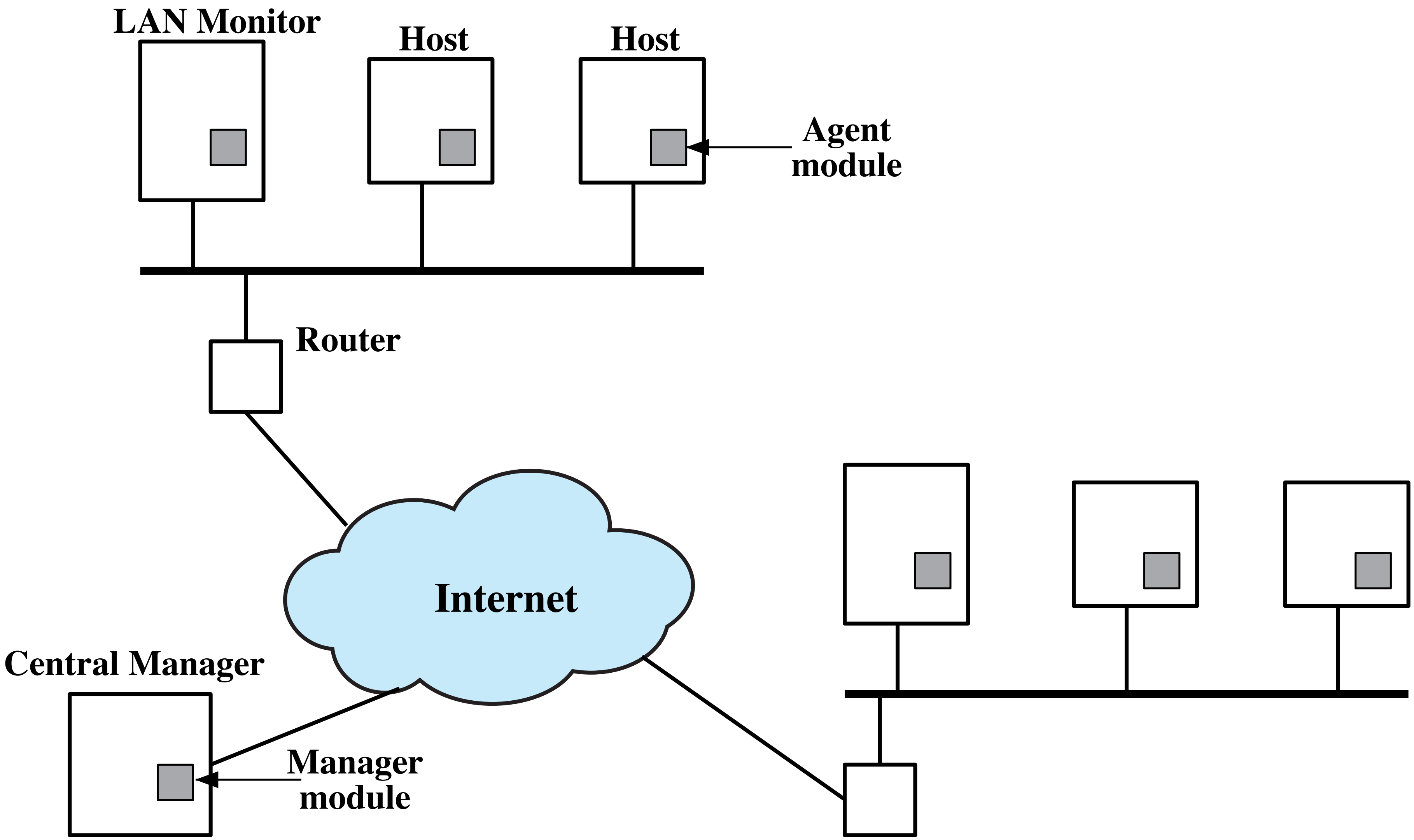


Figure 8.2 Architecture for Distributed Intrusion Detection

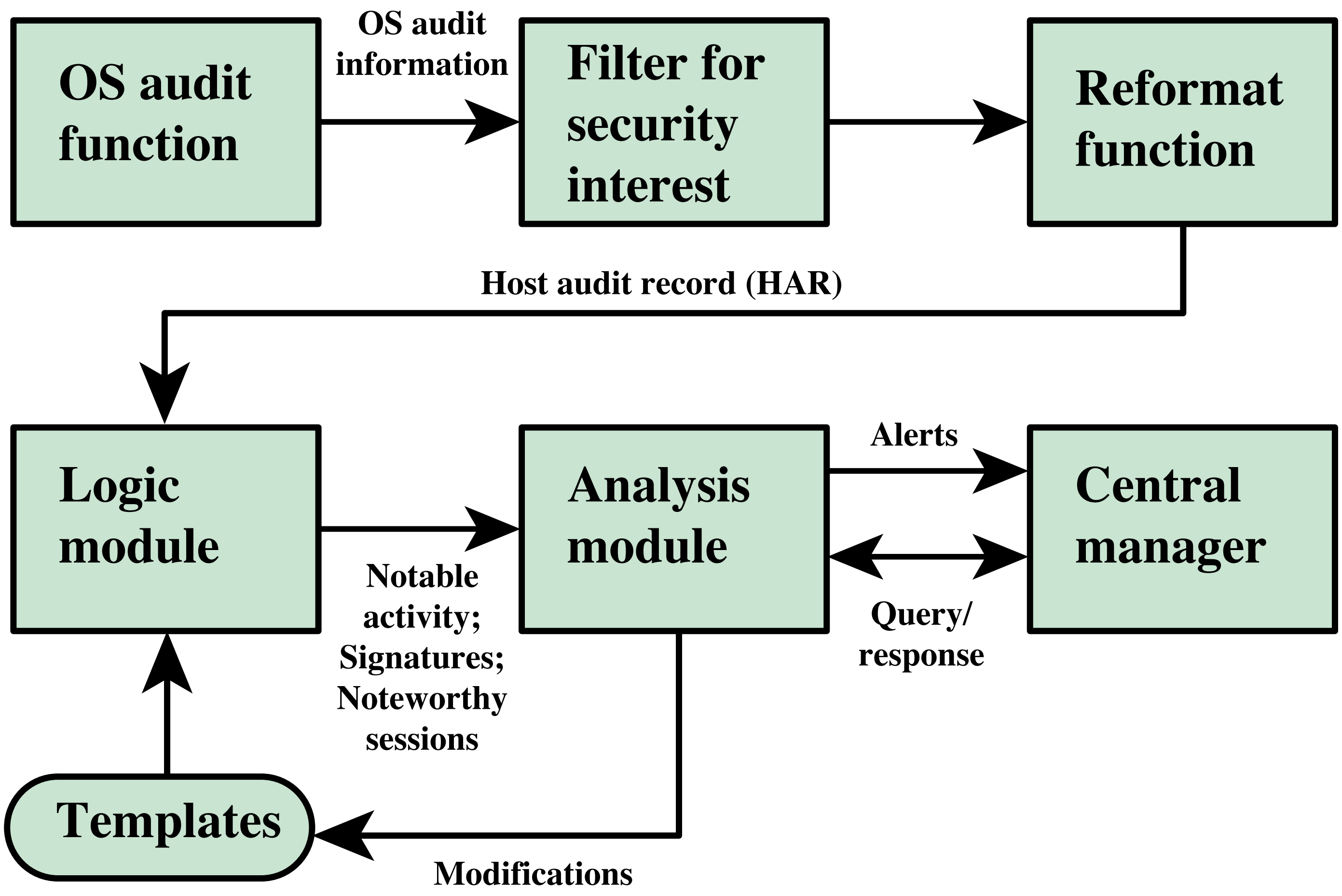


Figure 8.3 Agent Architecture

Network-Based IDS (NIDS)

Monitors traffic at selected points on a network

Examines traffic packet by packet in real or close to real time

May examine network, transport, and/or application-level protocol activity

Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

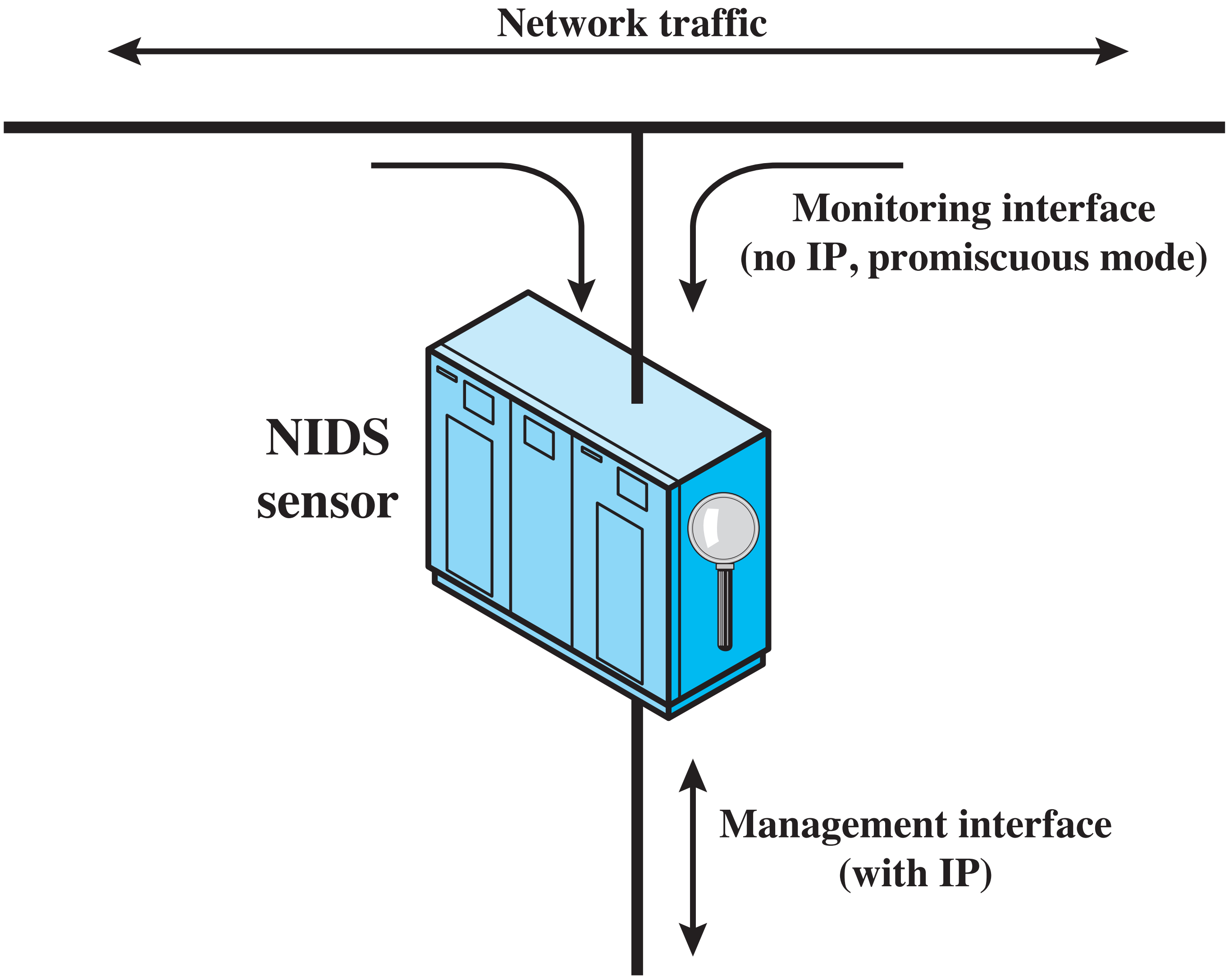


Figure 8.4 Passive NIDS Sensor

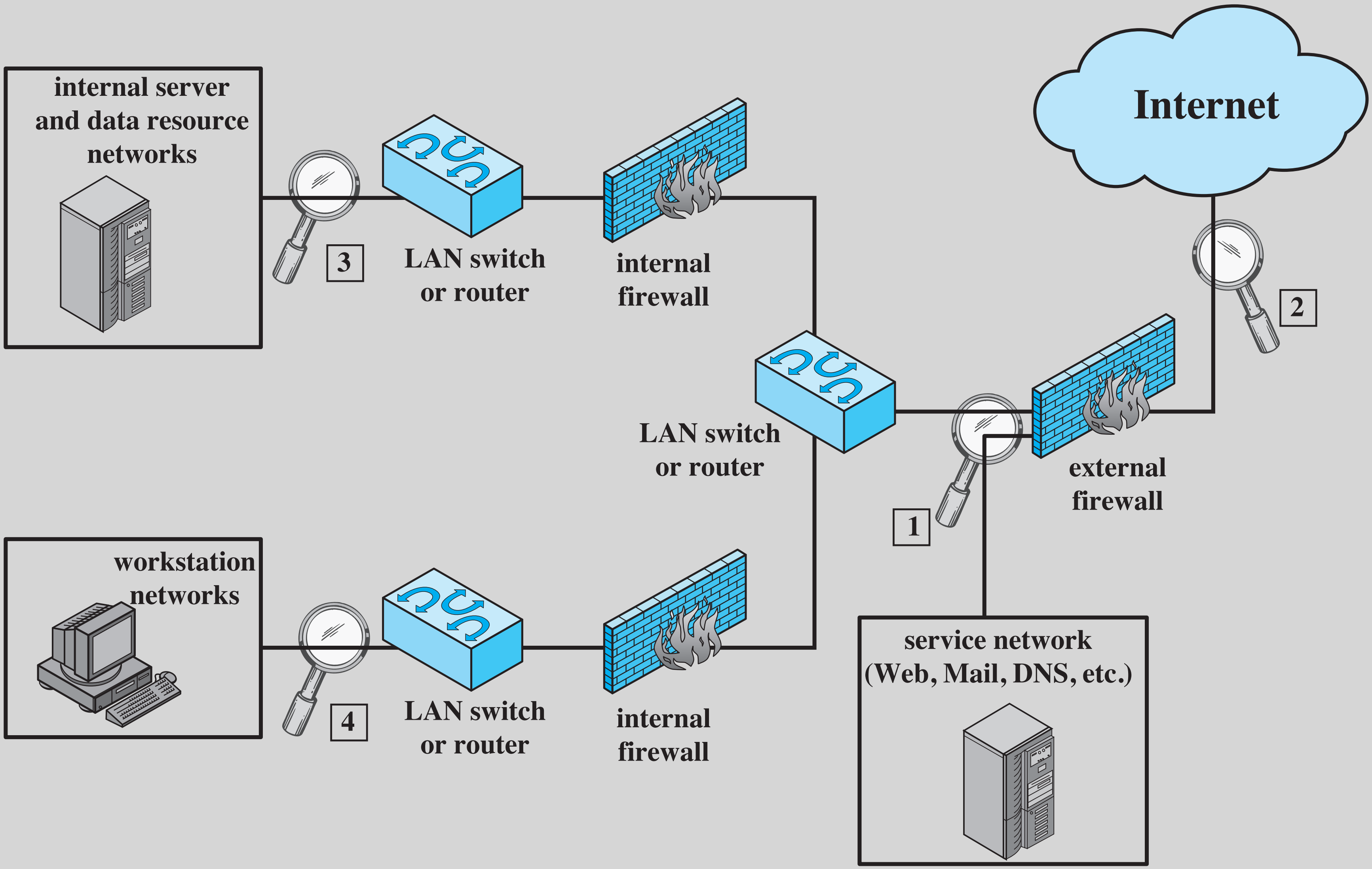


Figure 8.5 Example of NIDS Sensor Deployment

Heilmeier Questions

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you succeed, what difference will it make?
- What are the risks?
- How much will it cost?
- How long will it take?
- What are the mid-term and final “exams” to check for success?