NSCOM01

UDP-Based Application Protocols

3rd Term– AY2022 – 2023

Instructor: Dr. Marnel Peradilla

USER DATAGRAM PROTOCOL

- **The User Datagram Protocol (UDP) is a connectionless transport protocol used in TCP/IP networks**
- **Considered as a 'bare-bones' protocol that provides only the essential capabilities needed to transport a data segment between applications**
- **Features:**
  1. Unreliable – datagrams are not acknowledged
  2. No congestion control mechanism- datagrams sent as quickly as possible
  3. Stateless – Server does not keep track of status and session information of a client. Each request-response exchange with a client is treated as an independent transaction
  4. Unordered delivery – datagrams do not contain any sequencing information

WHEN TO USE UDP

- **Connectionless services are commonly used with applications where occasional data loss is tolerable in exchange for reduced protocol overhead:**
  1. Inward Data Collection – periodic sampling of data sources such as sensors or automatic self-test reports from network equipment
  2. Outward Data Dissemination – message broadcasting to nodes or distribution of data to a network
  3. Request – Response – query-based applications that use a transaction service provided by a single server where a single request-response is typical
  4. Real-time applications – applications with a degree of redundancy or real-time requirement e.g. voice, telemetry

APPLICATION PROTOCOLS

- **Several well-known application protocols use UDP as transport protocol to support their operations:**
  - System Logging Protocol
  - Network Time Protocol
  - Domain Name System
  - Dynamic Host Configuration Protocol
  - Trivial File Transfer Protocol
  - Simple Network Management Protocol

SYSLOG

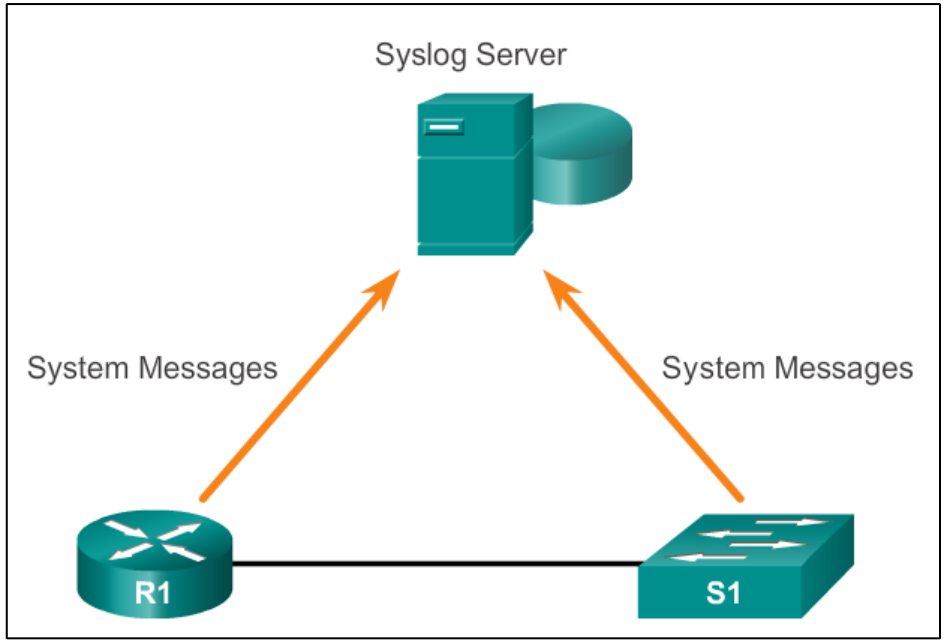
System Logging Protocol

INTRODUCTION TO SYSLOG

- **Monitoring an operational network is necessary**
  - Manage the network
  - Report network usage
  - Report any errors / problems that occur during operation
- **Information collection allows network administrators to collect event reports from devices for monitoring and future analysis.**
  - Provide trail of device activity
  - Early failure or operational error detection
  - Security incident detection and investigation
  - Project future growth
  - Regulatory compliance
  - Etc.

INTRODUCTION TO SYSLOG

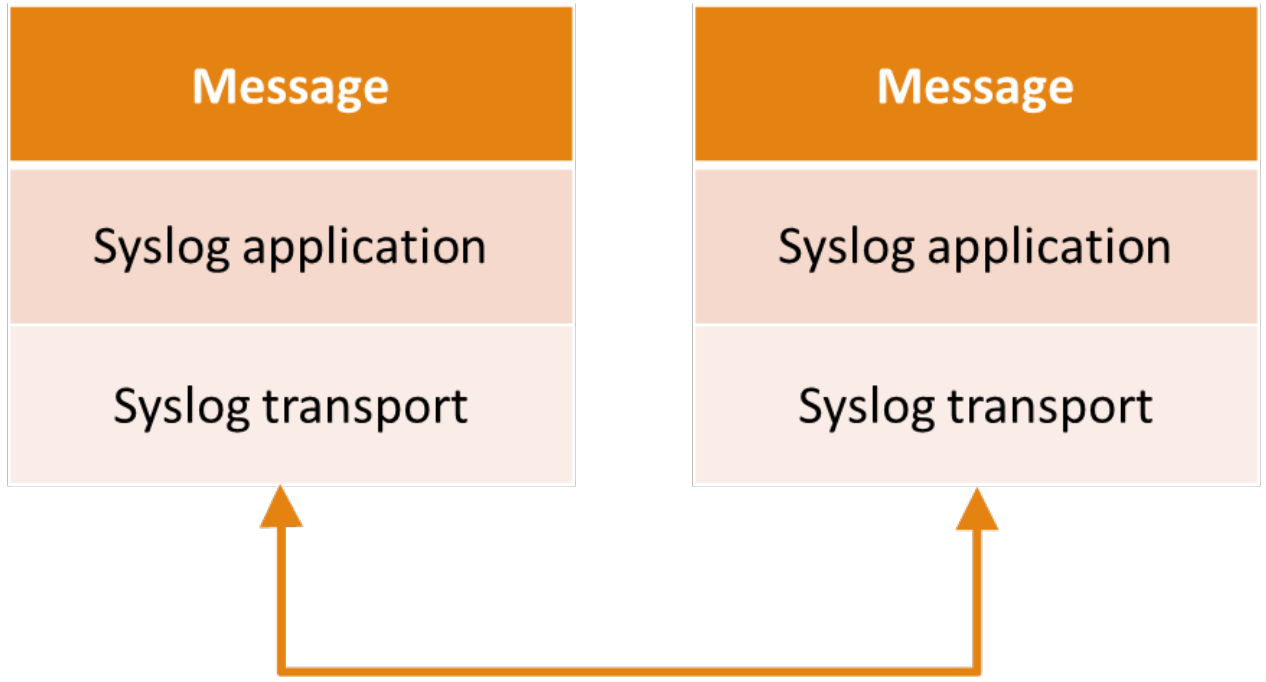
- **Syslog is a protocol that provides a to collect event notification messages from devices**
  - To a log file stored locally on the device,
  - Across the network to a socket on a remote logging server
- **Defines a common message format to allow a method of interpreting messages from devices from different vendors**
- **Protocol is described in RFC 3164 then later replaced by the proposed standard RFC 5424**



SYSLOG ARCHITECTURE

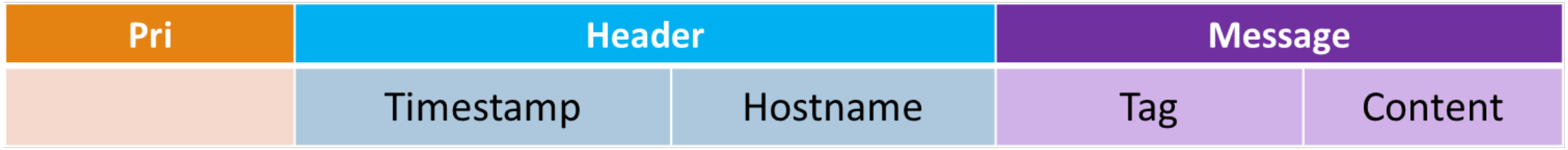
❑ Syslog utilizes three layers:

- "syslog content" is the management information contained in a syslog message.
- The "syslog application" handles generation, interpretation, routing, and storage of syslog messages.
- The "syslog transport" puts messages on the wire and takes them off the wire through a chosen transport layer protocol.



SYSLOG MESSAGE FORMAT (RFC3164)

- **Syslog messages are at least 480 bytes in length**
- **Messages contain the following:**
  - Pri – Message priority enclosed in <>
  - Header – Essential message details
  - Message Text - message details using a free-format content customized according to manufacturer of device



SYSLOG MESSAGE PRIORITY

- Syslog message priority facility code represents the type of program or component that generated the message
- Priority = facility_code * 8 + severity level

Code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16–23	local0 – local7	Locally used facilities

SYSLOG MESSAGE PRIORITY

- Syslog message severity represents criticality of messages
- Lower number indicates more critical event

Level	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug	Debug-level messages

SYSLOG MESSAGE FORMAT (RFC3164)

- **Header**
  - Timestamp - Mmm dd hh:mm:ss fomat
  - Hostname – hostname or IP address
- **Message**
  - Tag – contains process name and sometimes process ID, terminated by a non-alphanumeric character
  - Content – message body
- **Example**

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

SYSLOG MESSAGE FORMAT (RFC5424)

- **Syslog messages are at least 480 bytes in length**
- **Messages contain the following:**
  - Header – ASCII encoded containing mandatory and essential information about a message, very structured in format
  - Structured Data – mixed ASCII and UTF-8 encoded containing key-value pairs providing more details regarding a message.
  - Message Text - free-format content customized according to manufacturer of device

SYSLOG HEADER FIELDS

- **Priority – Comprises a facility code and severity level, enclosed in <> computed in the same way as RFC 3164**
- **Version – currently 1**
- **Timestamp – When the message was generated. Uses YYYY-MM-DDThh:mm:ss.sTZD format (Example: 1994-11-05T08:15:30-05:00 or 1994-11-05T13:15:30Z)**
- **Hostname – machine that sent the message identified using its fully qualified domain name (FQDN), IP address or hostname**
- **Application Name - identifies the device or application that originated the message.**

Header						
Priority	Version	Timestamp	Hostname	Application Name	Process ID	Message ID

SYSLOG HEADER FIELDS

- **Process ID - process name or process ID associated with a syslog system**
- **Message ID – Identified the message type – commonly used for filtering purposes at the collector**

Sample:

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog 12875 ID47 [exampleSDID@32473 iut="3"
eventSource="Application" eventID="1011"] BOMAn
application event log entry...
```

SYSLOG MESSAGE TEXT

- **Message text is an optional field containing ASCII or UTF-8 encoding (when preceded by characters 'BOM'**

Sample:

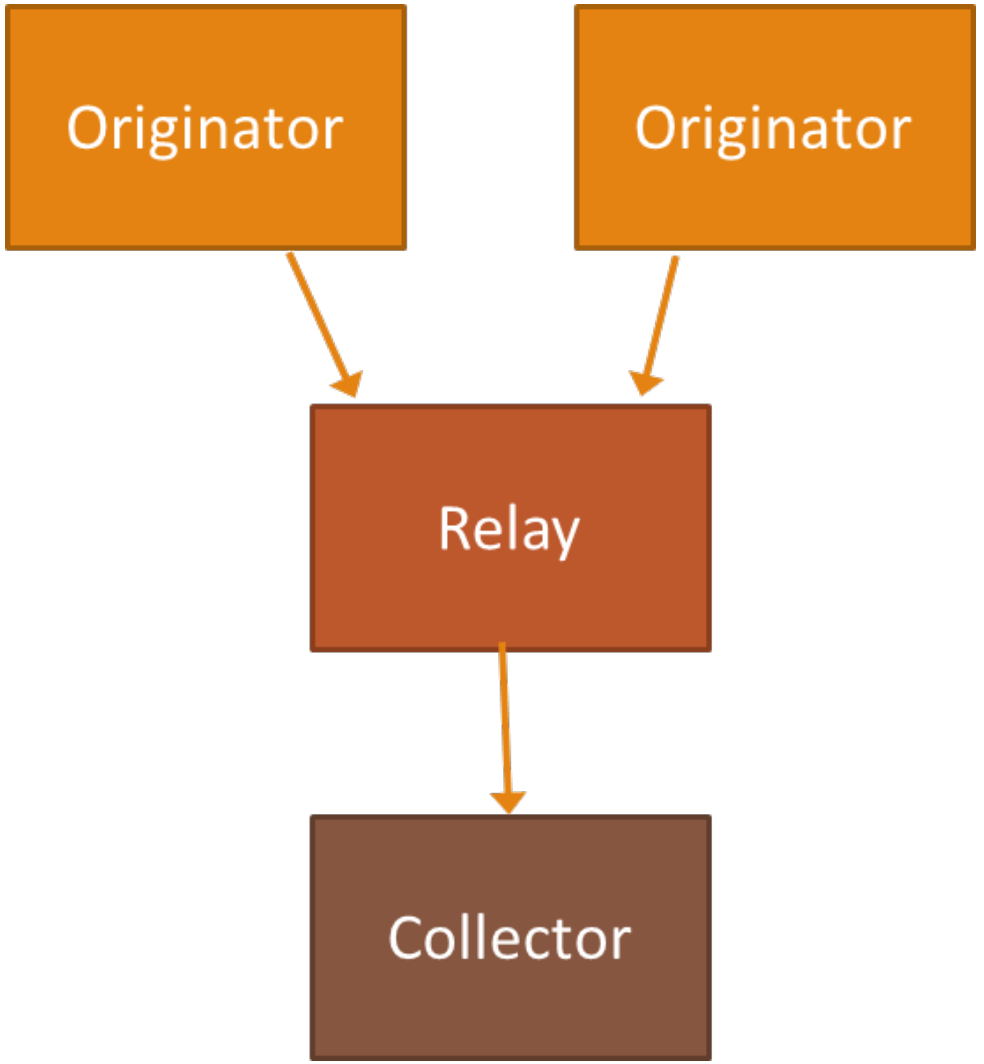
```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog 12875 ID47 [exampleSDID@32473 iut="3"
eventSource="Application" eventID="1011"] BOMAn application
event log entry...
```

SYSLOG DEPLOYMENT

❑ Functionalities

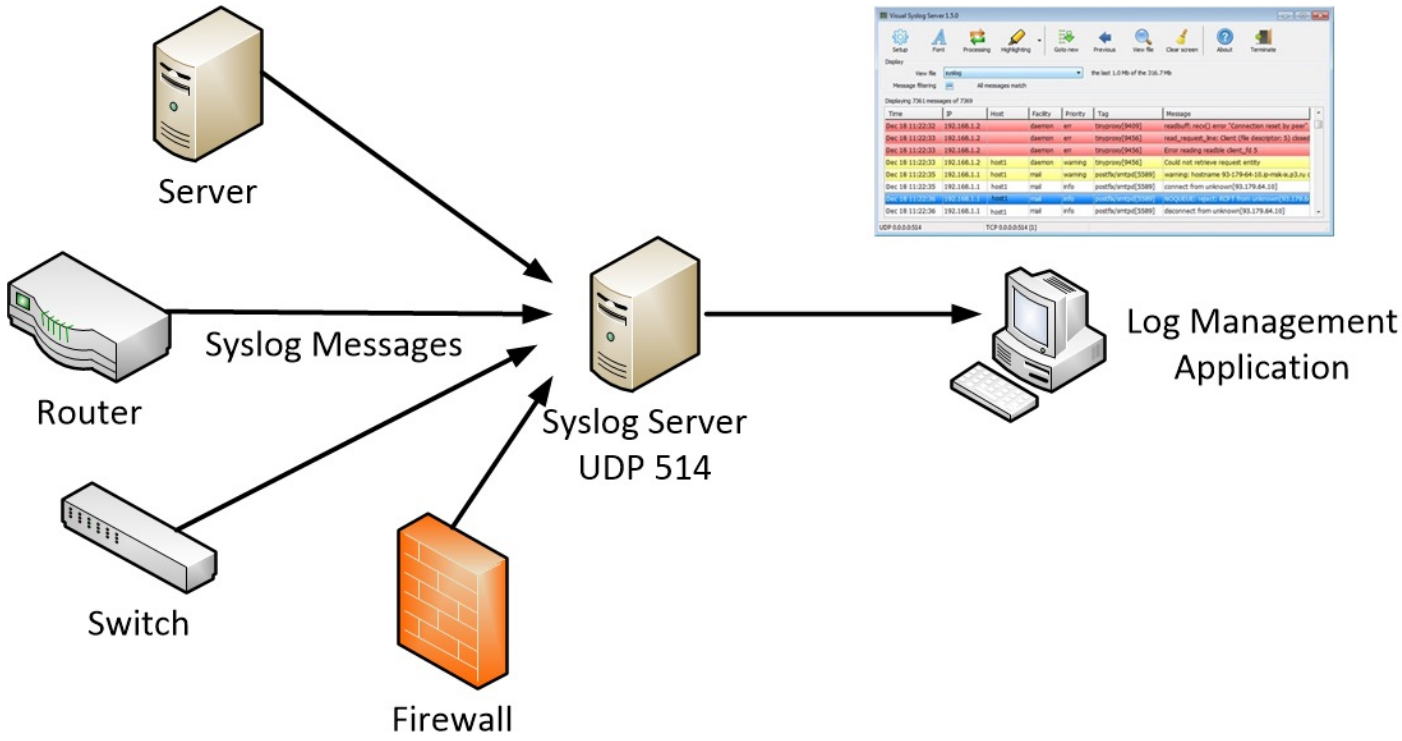
- An "originator" or “sender” generates syslog content to be carried in a message.
- A "collector" gathers syslog content for further analysis.
- Optional "relays" accept messages from originators or other relays and sending them to collectors or other relays.

❑ All 3 functionalities may reside on the same physical system



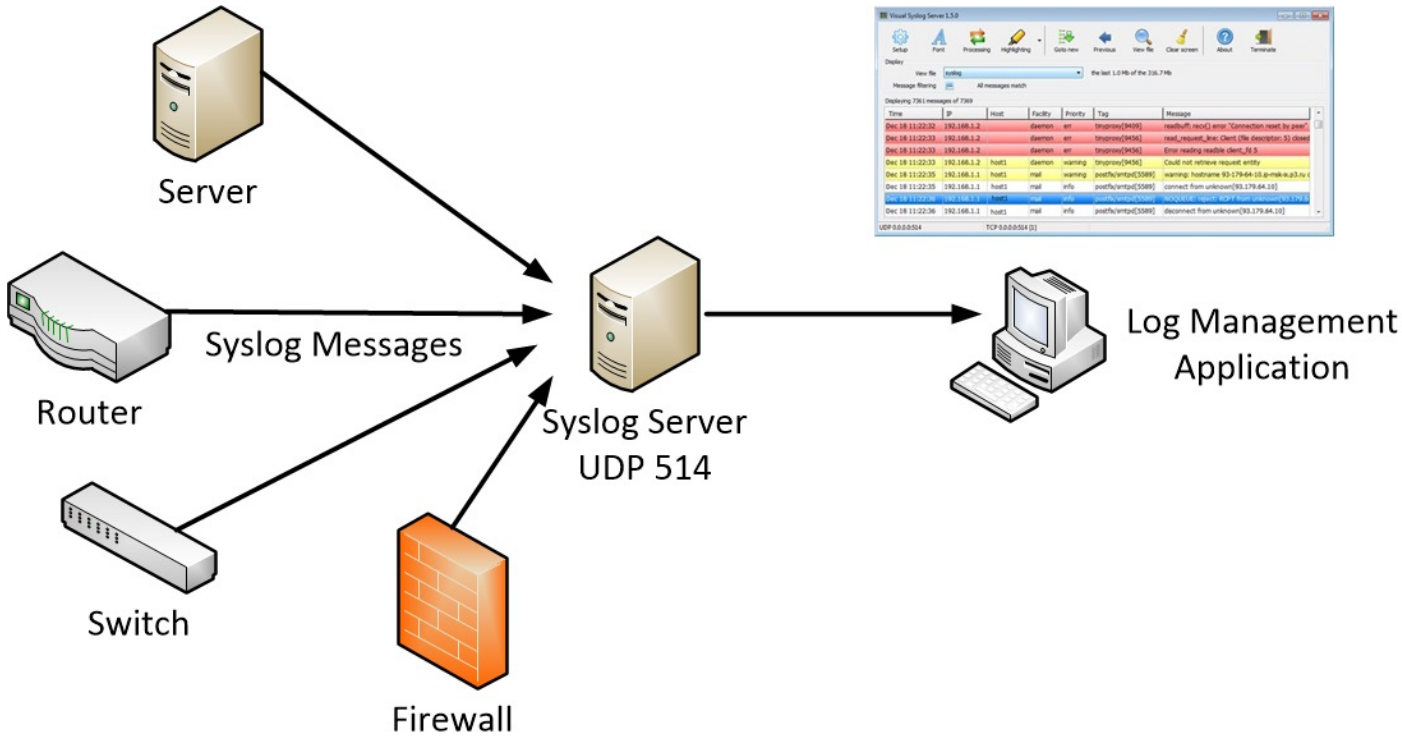
TYPICAL DEPLOYMENT SCENARIO

- Originators may be any network capable device with logging functionality
- Collector is a syslog server application listening on UDP port 514
- Syslog server process is a software that consolidates received log entries for network administrators to access for review through a user-friendly interface



TYPICAL DEPLOYMENT SCENARIO

- Optional relays may be placed between originator and collector, commonly for filtering based on severity, message ID, etc
- Originators may send to 1 or more relays or collectors, and relays/collectors may receive from 1 or more originators



LIMITATIONS

- **Although a proposed standard exists, a large number of devices still use the 3164 format (now classified as an obsolete RFC)**
- **Communication is simplex only. Messages are sent without acknowledgments hence message loss and dropping due to rejected content is possible**
- **No congestion control – Possible to overwhelm the collector**
- **No authentication – Possible to collect crafted and replayed messages**
- **No confidentiality – Messages sent in plain text**
- **If these features are needed for reliable and secure logging:**
  - Syslog over TCP (reliability) – RFC 6587
  - Syslog over TLS (security) – RFC 5425

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."