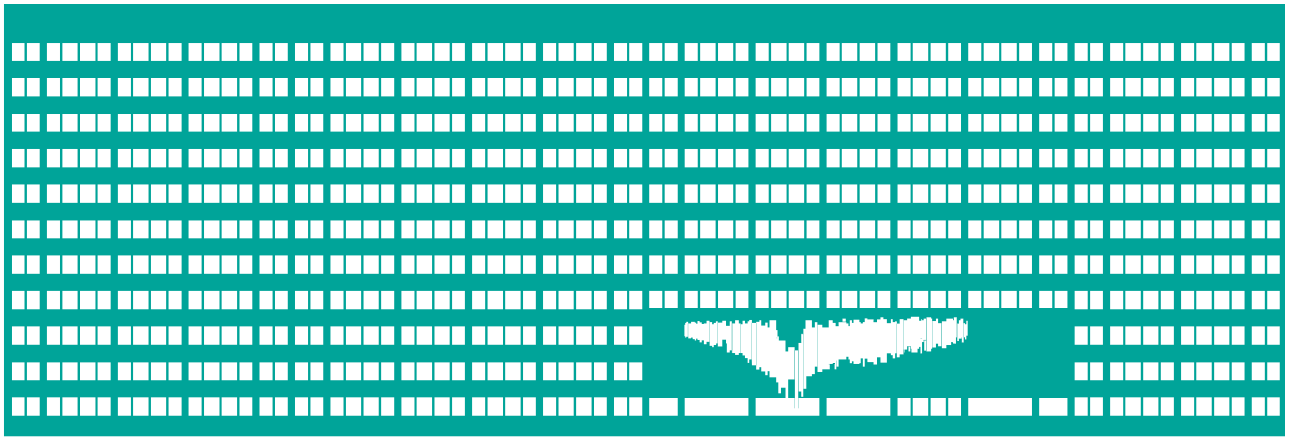
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Network System Services



Computer Networks
Lecture 11

Syslog

Syslog

- Aggregates logged messages from multiple network devices on the common logging server
  - Easier event lookup and evaluation of relations between consequent events
- Syslog server – a plenty of implementations (syslogd)
  - Supports both local and remote logging
  - May be configured to take an action after reception of specified message type
- Various log browsing and event correlation analysis frontend programs are available

Syslog Facilities

- The source client component (program) is defined using Facility
  - A set of facility values is predefined for most used system components
  - LOG_USER and LOG_LOCAL0-LOG_LOCAL7 may be used for custom components

Syslog Severity Levels (1)

- Severity level defines the message urgency
  - LOG_EMERG
    - system is unusable
  - LOG_ALERT
    - action must be taken immediately
  - LOG_CRIT
    - critical conditions
  - LOG_ERR
    - error conditions
  - LOG_NOTICE
    - normal, but significant, condition

Syslog Severity Levels (2)

- LOG_INFO
  - informational message
- LOG_WARNING
  - warning conditions
- LOG_DEBUG
  - debug-level message (very detailed)

Structure of Syslog Message

- Timestamp
  - All network components have to have synchronized time to make Syslog messages meaningful and correlations analysis possible
- Severity
- Facility
- [PID]
- Description text

Syslog Protocol

- Syslog protocol is standardized in RFC 3164
  - Uses UDP or TCP transport
- Messages are sent as cleartext
  - May be secured by wrapping into SSL
- Syslog server may intelligently sort received messages into multiple files according to predefined rules
- Syslog servers may be chained
  - Intelligent filtering and forwarding of selected messages

Programming of Syslog-aware Applications

- Client-side libraries are available for most programming languages
  - C, Perl, Bash, ...
  - System calls for sending a message to syslog daemon
    - passed either on the local syslogd or forwarded to configured central syslog server
    - Bitmask specifying what severity levels should be logged may be programmed

Network Time Protocol (NTP)

Network Time Protocol (NTP)

- Protocol used to synchronize clocks of network-attached devices over a packet network with variable transport delay
  - RFC 5905 (NTPv4) + extensions
  - Transported over UDP/123
- Utilizes (hierarchy of) NTP servers
  - NTP clients ask NTP servers for the precise time
  - available as NTP daemon or library
- Achievable accuracy:
  - Internet: 10ms
  - LAN: 200 us

NTP Usage

- Maintaining of servers' system clock
- Maintaining of user computers' system clock
- Maintaining the network infrastructure devices' clock
  - Security technologies (certificates, anti-replay mechanisms, ...)
  - Real time for system event logging
  - Time-based ACL
  - ...

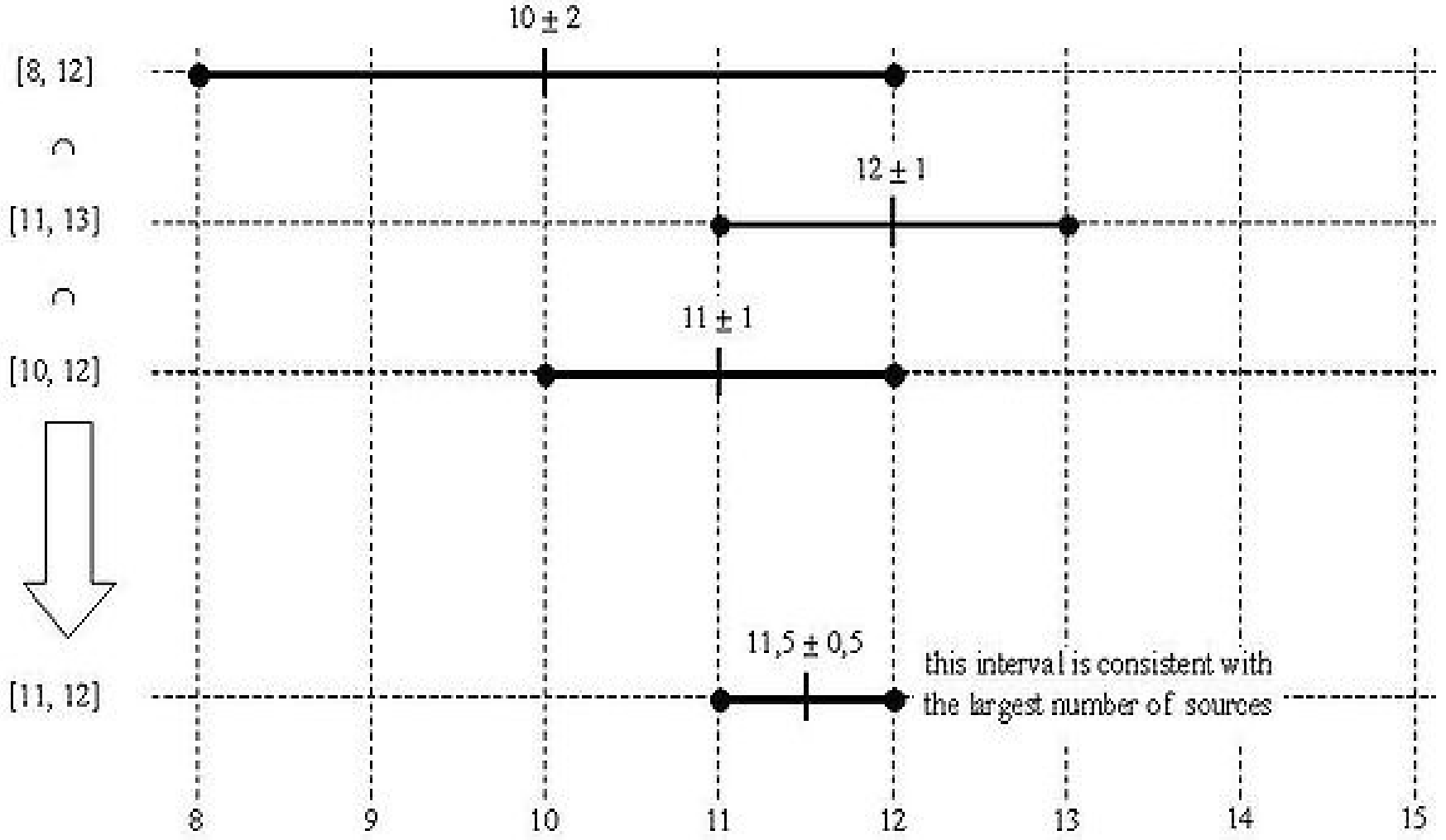
Time Representation in NTP

- NTP Works with UTC
  - 32-bit seconds + 32-bit fractional second part
    - Relative to January 1, 1900
    - wraps around every 136 years
    - applications may use other clock source to remove the ambiguity
    - no roll-over problem as NTP uses relative timestamps
  - 64-bit signed seconds + 64-bit fractional part possible
    - 32-bit era number + 32-bit seconds (same as above)
- Time zones and daylight saving time have to be handled separately

Clock Calculation in NTP

- Marzullo's algorithm is used to calculate the clock
  - Produces an optimal value from a set of estimates with confidence intervals
  - Asymmetric routing between client and server makes troubles (different path with different delays)
- Transport delays are calculated from timestamps placed by client and server into the NTP messages

Marzullo's algorithm

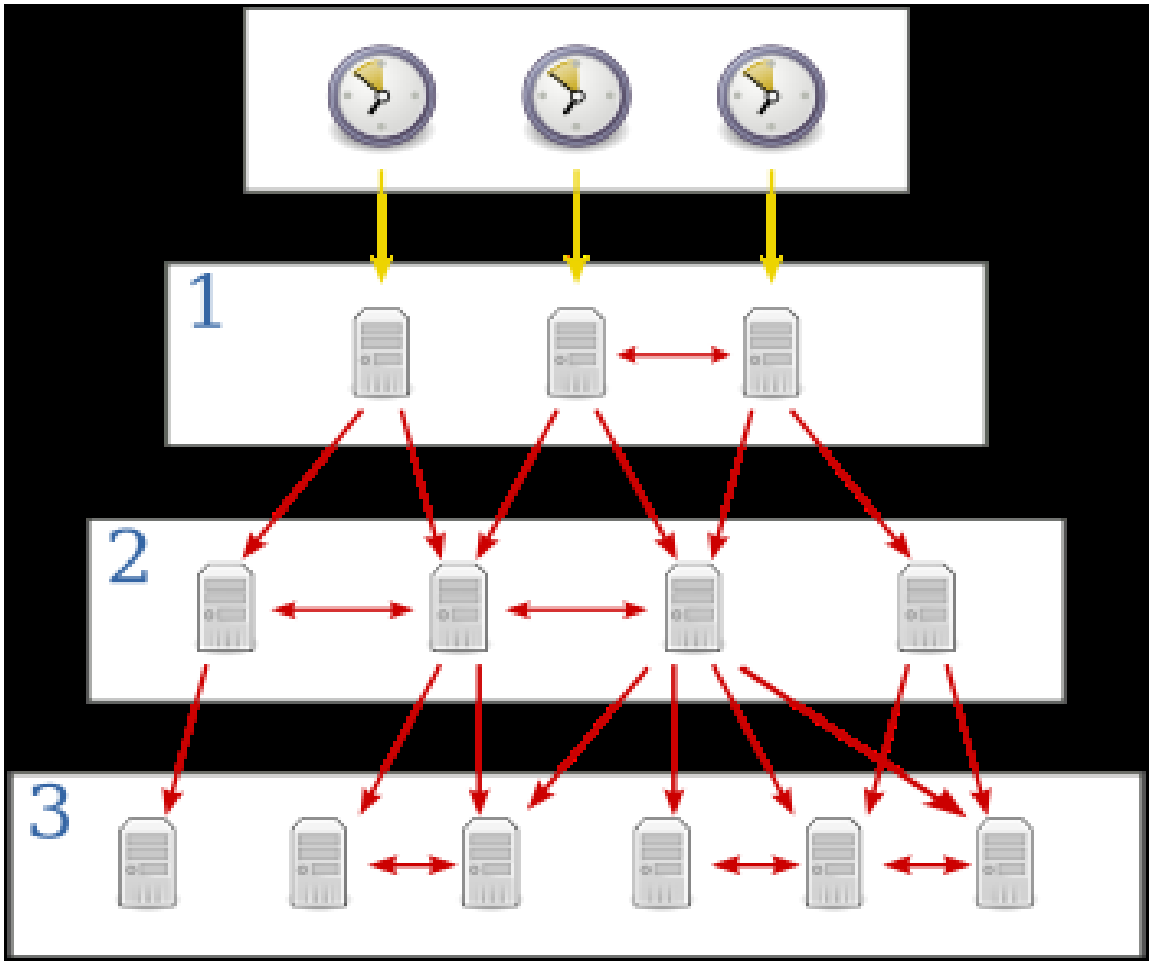


See http://en.wikipedia.org/wiki/Marzullo%27s_algorithm for details

NTP Clock Sources Hierarchy

- NTP uses hierarchical system of clock sources
  - Each layer corresponds to a stratum number (0=root)
    - Stratum defines the distance from the top
      - Used to prevent cycles in the hierarchy
      - Stratum is NOT an indication of quality or reliability
- Distributes client requests over multiple clock sources (load balancing)
- Avoids the dependency on the single clock source

NTP Strata (1)



Picture from http://en.wikipedia.org/wiki/Network_Time_Protocol

NTP Strata (2)

- Stratum 0
  - atomic clocks, GPS clocks, radio clocks
- Stratum 1
  - Time servers attached to Stratum 0 devices.
  - Process timing requests
- Stratum 2,3
  - computers that send NTP requests to Stratum N-1 server
  - peer with other Stratum 2 computers to provide more precise for all devices in the peer group

Simple Network Time Protocol (SNTP)

- Less complex
  - inter-operable with NTP, but uses simpler algorithm
- Less accurate
  - clients normally use only one SNTP server
    - supposes constant transport delay
- Used in some embedded devices
- Recommended only for the leaves of the NTP hierarchy

AAA Servers

Authentication, Authorization and Accounting (1)

- Authentication
  - verification of the identity of user who tries to access the network
- Authorization
  - Determining whether the particular user's activity should be allowed or denied
    - attaching to the network from particular NAS
    - entering particular configuration command into a given network device
    - ...

Authentication, Authorization and Accounting (2)

- Accounting
  - Helps to keep track of user's activities
    - security and legal reasons
  - Records may be used for billing

Remote Authentication Dial-In User Service (RADIUS)

- Standardized in RFC 2865 + 2866 (Accounting)
- Authenticates clients connecting to the NAS
  - WiFi, AP 802.1x-enabl. Ethernet switch, dial-in server, ...
- Supports various authentication methods
  - User name + password (CHAP style), certificates, ...
  - One-way or mutual authentication
- Accounting support
  - Logs information about session start and session termination
- May act in proxy mode
  - e.g. EduROAM
- Works over UDP/1812 (authentication) and UDP/1813 (accounting)

Lightweight Directory Access Protocol (LDAP)

- Protocol for accessing data stored on the directory server
  - Simplifies CCITT X.500 DAP standard
- The purpose of directory server is to maintain a central storage of information related to network users
- Objects with various attributes are organized into a tree structure
  - Hierarchical system of containers
- The LDAP scheme that defines object classes and their attributes may be customized to maintain custom attributes