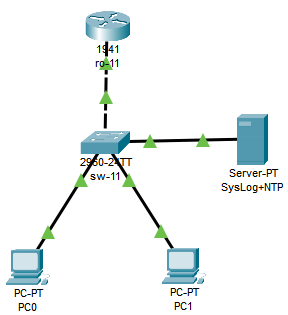
## Лабораторная работа №11. SysLog

**syslog** (англ. *system* *log* — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания событийных журналов), использующийся в компьютерных сетях, работающих по протоколу IP. Термином «syslog» называют как ныне стандартизированный сетевой протокол syslog, так и программное обеспечение (приложение, библиотеку), которое занимается отправкой и получением системных сообщений.

Стандартом предусматривается, что источники формируют простые текстовые сообщения о происходящих в них событиях и передают их на обработку серверу Syslog, используя один из сетевых протоколов семейства IP (UDP или TCP). Формирование сообщений о событиях и их передача происходит по определённым правилам, называемым протоколом Syslog. Как правило сообщение имеет небольшой размер (до 1024 байт) и отсылается в открытом виде. Поскольку источники сообщений и сервер Syslog могут располагаться на разных машинах, это позволяет организовать сбор и хранение сообщений от множества географически разнесённых разнородных источников в едином хранилище (репозитории), что чрезвычайно важно для администраторов сетей, которые могут и не иметь физического доступа сразу ко всем устройствам и компьютерам в сети.

Текущая версия протокола Syslog предлагает усовершенствованный формат сообщений, позволяющий использовать точную отметку времени создания сообщения и осуществлять надежную идентификацию источника сообщения, а также применять кодировку UTF-8 для текста сообщения, что позволяет решить проблему интернационализации. Необязательные дополнительные поля (структурированные данные) могут использоваться для передачи различной информации, например, о погрешности локальных часов источника сообщения и точности их синхронизации с внешними часами точного времени, о языке, на котором написано сообщение, и т. д.



1. Расставим оборудование
   * Маршрутизатор Cisco 1941
   * Коммутатор Cisco 2960
   * Сервер
   * Несколько рабочих станций
2. Соединим оборудование
   * Соединим активное оборудование по гигабитным портам
   * Присоединим конечные устройства к коммутатору по портам FastEthernet.
3. Настройка сервера
   * Спланируем распределение статических и динамических IP-адресов
   * Настроим статический адрес сервера. Укажите шлюз по умолчанию
   * Настроим службу DHCP. Укажите начало диапазона динамических адресов и шлюз по умолчанию
     + Убедитесь, что рабочие станции получают корректные настройки IP
   * Убедитесь, что служба Syslog по умолчанию включена
4. Настройка маршрутизатора
   * Задайте имя
   * Задайте IP-адрес
     + interface GigabitEthernet0/0
     + no shutdown
     + ip address 192.168.108.1 255.255.255.0
   * Настройте сбор логов по протоколу syslog на сервер:
     + logging on
     + logging trap debugging
     + logging 192.168.108.20
   * Проверьте вывод команды show logging
   * Убедитесь, что логи направляются на сервер, но время сообщения указывается некорректно
   * Настройте отправку времени командой service timestamps log datetime msec
   * Убедитесь, что время указывается корректно, но текущее время на маршрутизаторе (show clock) не настроено
5. Настройка службы точного времени NTP
   * Убедитесь, что служба NTP включена на сервере по умолчанию
   * Подключите маршрутизатор к службе: ntp server 192.168.108.20
   * При помощи команд show ntp проследите за процессом подключения и установки времени
   * Убедитесь, что логи направляются на сервер с корректным временем
6. Настройка коммутатора
   * Задайте имя
   * Задайте IP-адрес
     + interface Vlan1
     + no shutdown
     + ip address 192.168.108.10 255.255.255.0
   * Подключите коммутатор к службе точного времени: ntp server 192.168.108.20
   * Настройте сбор логов по протоколу syslog на сервер:
     + logging on
     + logging trap debugging
     + logging 192.168.108.20
   * Настройте отправку времени командой service timestamps log datetime msec
   * Проверьте вывод команды show logging
   * Убедитесь, что логи направляются на сервер с корректным временем
7. Сохраните файл и отправьте его на оценку
   * Не забывайте про необходимость документирования сети

## Приложение

Настройки сетевого оборудования

hostname **sw-11**

interface GigabitEthernet0/0

ip address 192.168.108.1 255.255.255.0

no shutdown

logging trap debugging

logging 192.168.108.20

service timestamps log datetime msec

ntp server 192.168.108.20

hostname **sw-11**

interface Vlan1

ip address 192.168.108.10 255.255.255.0

no shutdown

logging trap debugging

logging 192.168.108.20

service timestamps log datetime msec

ntp server 192.168.108.20