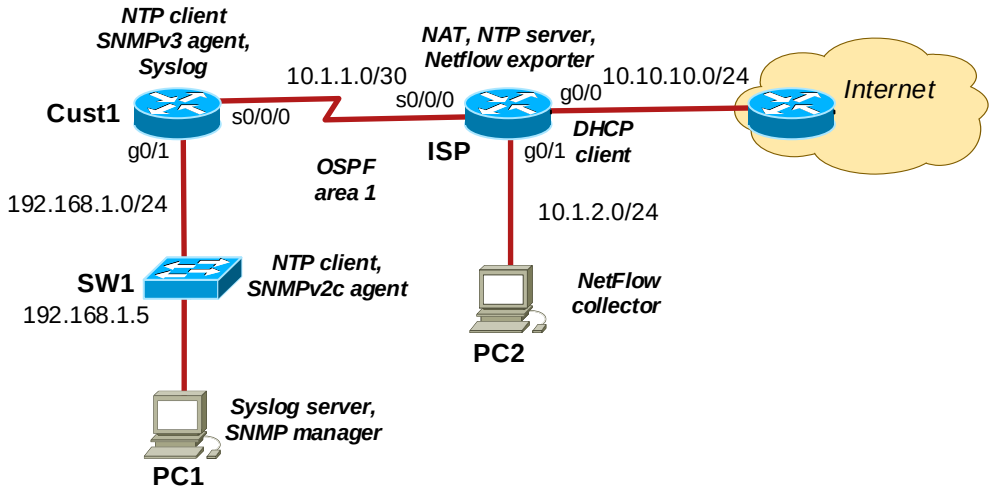
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

CCNA R&S 4

Network Monitoring 1/2



Scenario — Monitoring Network Using Syslog, SNMP and NetFlow.

Configure monitoring using syslog, SNMP and NetFlow for a local network connected to the Internet. Monitoring of a local customer network (router Cust1, switch SW1) is implemented using SNMP and syslog. Monitoring data is forwarded to the PC1. ISP provides its own traffic monitoring using Netflow. Netflow exporter is implemented on ISP router, records are sent to the collector on PC2.

Task 1 — Configure Basic Device Settings.

1. **Prepare your network.**
   Step 1: Cable network topology.
   Step 2: Clear all existing configurations.
2. **Perform basic router configuration.**
   Configure the router and switch hostnames to match the topology diagram.
   Disable DNS lookup.
3. **Configure serial connection between R1 and R2.**
4. **Configure IP addresses and routing.**
   Configure IP addresses on all interfaces.
   PCs in LAN will receive configuration settings using DHCP server on Cust1 and ISP. Exclude the first 10 IP addresses for special purposes. Set DNS server address to 10.10.10.1.
   Configure static address 192.168.1.5 on SW1.
   ISP is connected to the Internet via Ethernet interface. Its IP address is obtained by DHCP.
   Configure NAT enabling access to the Internet for all local networks.
   Enable OSPF area 1 on the routers for all networks. Do not advertise routes to the Internet or LANs.
4. **Verify connections.**
   Test connection between all devices and towards the Internet.
   Test connection from PCs to all active network devices.

Task 2 — Configure NTP Synchronization.

Configure ISP as the NTP server and Cust1 and SW1 as NTP clients.

1. **Display the current time on ISP, Cust1, SW1.**
   router# show clock
2. **Set manually the reference time on ISP.**
   router# clock set *<hh:mm:ss> <day> <month> <year>*
3. **Configure NTP master on ISP. Use stratum 1. Stratum is the number of NTP hops away from an authoritative time source.**
   router(conf)# ntp master <stratum>
4. **Verify IP connection between ISP, Cust1 and SW1.**
5. **Configure the NTP client on Cust1 and SW1. Set periodical updates of the calendar with NTP time.**
   router(conf)# ntp server *<IP-address>*
   router(conf)# ntp update-calendar ; on router only
6. **Verify NTP status and NTP associations. Initial synchronization can take about 10 minutes.**
   router# show ntp status
   router# show ntp associations
7. **NTP synchronization can took time. Use debugging to see NTP messages.**
   router# debug ntp events/packets

Task 3 — Configure Syslog Logging.

Start the syslog server on PC1. Configure syslog logging on Cust1.

1. **Start Tftpd64 application on PC1. Set TFTP server interface on 192.168.1.0/24 network. Switch to the Syslog panel.**
2. **Configure Cust1 to log messages to the syslog server.**
   router(conf)# logging host *<IP>*
3. **Display the default logging settings. What is the IP address of the syslog server? What protocol and port is used by syslog?**
   router# show logging
4. **Observe the various trap levels (severity levels) available.**
   router(conf)# logging trap ?
5. **Change the logging severity level to 4 (warnings).**
   router(conf)# logging trap warnings
6. **Create and delete interface loopback 1 on Cust1. Observe the log messages on both terminal window and the syslog console on PC1.**
   router(conf)# interface loopback 1
   router(conf)# no interface loopback 1
7. **Change the logging severity level to 6 (informational) and provide the same test with interface loopback 1.**
   router(conf)# logging trap 6

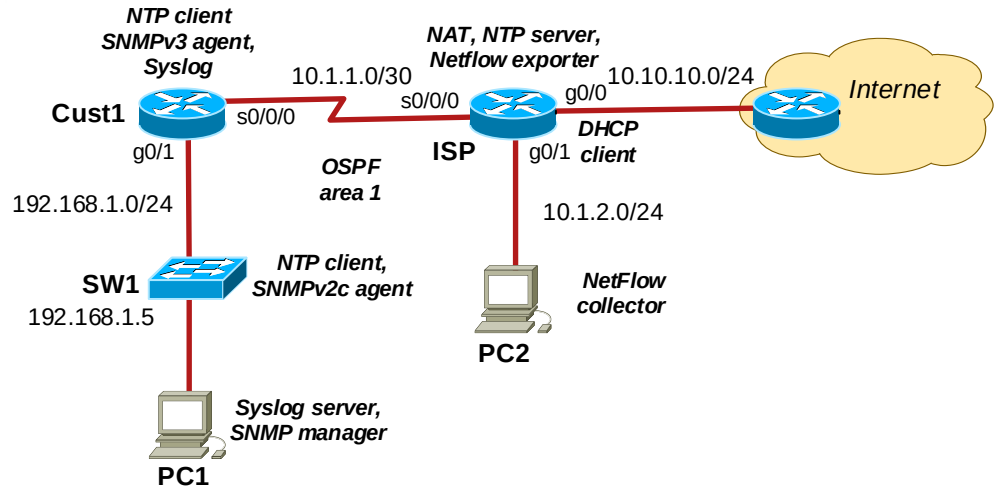
Task 4 — Installing SNMP Manager on PC1

Download SNMP MIB Browser from netacad.fit.vutbr.cz/CCNA Courses/CCNA4 and install it on PC1 if not installed yet.

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

CCNA R&S 4

Network Monitoring 2/2



Task 5 Configure SNMP Monitoring.

1. **On SW1, Configure an ACL limiting access to SNMP to PC1 only.**
   switch(conf)# ip access-list <no.> permit host <IP address>
2. **Configure a SNMPv2 agent on S1 with community string *ciscolab* for read-only access. Enable traps with the password *class123*.**
   switch(conf)# snmp-server community <community-string> ro <ACL-number>
   switch(conf)# snmp-server location <location>
   switch(conf)# snmp-server contact <contact>
   switch(conf)# snmp-server host <SNMP-server-IP> version 2c <community-string>
   switch(conf)# snmp-server enable traps
4. **Verify SNMP settings.**
   switch# show snmp
   switch# show running | include snmp
5. **Enable SNMP traps on the SNMP MIB Browser.**
   In the MibBrowser, click Edit/Settings. Verify that v2c version is selected.
   Open View/TrapViewer. Check if port 162 is correctly set. Configure the community string.
   Click Start to launch traps processing. If trap is received, click on Show details and check the type of the event.
   switch# conf t ; invoke a trap by switching to the configuration mode
6. **Browse MIB database of SW1.**
   Select the system group in RFC1213-MIB tree in the right column. Set the hostname and community string of SW1. Using Get SNMP variable icon retrieve MIB objects from the SNMP agent. Check the retrieved values.
7. **Configure a SNMPv3 agent on Cust1. Set an ACL to limit access to PC1 only. Configure SNMP view, access group *ADMIN* for read-only access, and SNMP user *User1* with password *cisco1234* for authentication using SHA and encryption using AES-128 algorithms if available.**
   router(conf)# snmp-server view SNMP-RO iso included
   router(conf)# snmp-server group ADMIN v3 priv read SNMP-RO access <ACL-no>
   router(conf)# snmp-server user User1 ADMIN v3 auth sha <passwd> pri aes 128 <passwd>
8. **Verify SNMP settings.**
   router# sh run | include snmp
   router# show snmp user
   router# show snmp community

Task 6 Testing SNMP Monitoring.

1. **Start Wireshark on PC1 to see SNMP and syslog communication.**
2. **Generate an SNMP trap and notification by putting an interface on down and up.**
   router(conf-if)# shutdown
   router(conf-if)# no shutdown.
3. **Browse MIB database of Cust1.**
   In SNMP MIB Browser, click on Edit/Settings. Select version v3 and click on Add. Configure IP address, username, and security level (Auth,Priv). Set proper authorization and encryption methods and passwords. Click OK to continue.
   Select interface MIB group in the right column of the MIB Browser and retrieved data using Get SNMP icon. Check the received values.
4. **Analyze encrypted SNMP data in Wireshark.**
   Select any packet with SNMPv3 communication in Wireshark. Right click on the packet and select Protocol preferences / Simple Network Management Preferences.
   Click Edit for the Users Table. Click + and enter user information about algorithms and keys. Click OK.
   Select one of the SNMPv3 packets again. Expand the SNMP result and view the decrypted message.

Task 7 Collecting and Analyzing NetFlow Data

1. **Configure NetFlow capture on the serial interface of ISP. Capture data in both directions.**
   router(conf-if)# ip flow ingress
   router(conf-if)# ip flow egress
2. **Configure NetFlow data export on NetFlow collector at PC2. Set port to 9995.**
   router(conf)# ip flow-export destination *<IP-address> <port>*
3. **Set NetFlow export version as version 5 or 9.**
   router(conf)# ip flow-export version <version>
4. **Verify the NetFlow configuration.**
   router# show ip flow interface
   router# show ip flow export
5. **Display a summary of the NetFlow accounting statistics: packet size distribution, IP flow information, captured protocols, number of total packet, etc.**
   router# show ip cache flow
6. **Check NetFlow data using Wireshark on PC2.**
   Set proper decoding of NetFlow packets in Wireshark. Use menu Edit/Preferences/Protocols/CFlow and add a new NetFlow UDP port.
7. **Verify NetFlow records.**
   Generate ICMP communication from PC1 to the outside network. Check how this flow is stored in the captured NetFlow records.

Task 8 Install Netflow Collector on PC2.

1. **Boot CentOS on PC2. Login using root/root4lab credentials.**
2. **Install nfdump collector using yum tool.**
   # yum install nfdump
3. **Disable the firewall on the system.**
   # systemclt stop firewall.service
4. **Create /data/netflow directory and start collecting netflow data using nfcapd daemon.**
   # nfcapd -t 120 -T all -S 7 -z -D -w -p <port> -l /data/netflow
5. **Start wireshark on PC2. Configure decoding flow records as CFlows.**
   Expand the flow records and analyze transmitted data.
6. **Analyze flow records stored in PC2 using nfdump. See man nfdump for filters.**
   /data/netflow # nfdump -R . -o line ; see all the records
   /data/netflow # ndfump -R . -o line -s dstip/packets ; see top N hosts based on destination IP.

Task 9 Finish the lab, remove cables, switch off PCs.