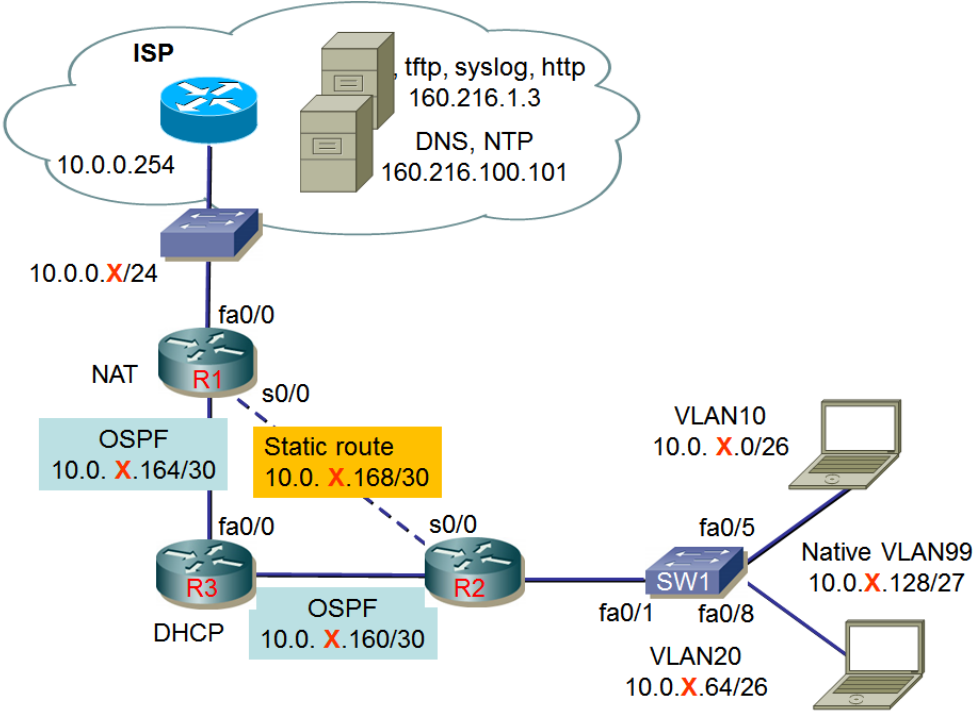


X=

CCNA7 ENSA – final

X – number of your
switch interface



Tasks:

1. Connect the network and set the addresses according to the topology above.
2. Protect local and remote access to routers and switches with passwords (`cisco`).
3. Protect the transition to privileged mode with a password (`class`).
4. Allow remote access only using SSH protocol (username `admin`, password `access`) .
5. Create VLANs on the switch, including a native VLAN (99).
6. Select the lowest possible IP addresses for routers and the highest possible IP addresses for stations.
7. Use OSPF routing protocol (it will propagate the default path information).
8. Routing will be authenticated by MD5 or SHA, password will be `smer123` .
9. The default path (toward ISP) will be set statically; do not propagate subnet 10.0.0.0/24 into OSPF.
10. Create backup static path between routers R1 and R2, which will only be used if the path through router R3 fails.
11. Router R1 will perform port address translation (NAT/PAT).
12. Router R3 will act as a DHCP server for the subnets connected to switch SW1 (DNS server is 160.216.100.101).
13. On all network devices, set the NTP server to 160.216.100.101
14. Save the router and switch configurations to the tftp server 160.216.1.3. The file names will consist of your last name and the device designation (e.g. Kaderka-R1).

Hints:

1. Connect devices, configure VLANs and set IP addresses (write in the picture above) firstly.
2. Then configure OSPF and verify functionality.
3. Next, configure and verify NAT/PAT.
4. Configure the DHCP server.
5. Find **any** solution to keep Internet available even in case of failure any of the links between the R3-R1 or R3-R2 routers.

6. Results evaluation

Basic setting

- Passwords on R1 ☐
- Passwords on R2 ☐
- Passwords on R3 ☐
- Passwords on SW1 ☐
- VLAN ☐
- OSPF ☐
- Remote SSH access ☐

Network backup setting

- Internet access in case of R3 or links R3-R1, R3-R2 failure ☐

DHCP

- Files are stored on the TFTP server ☐