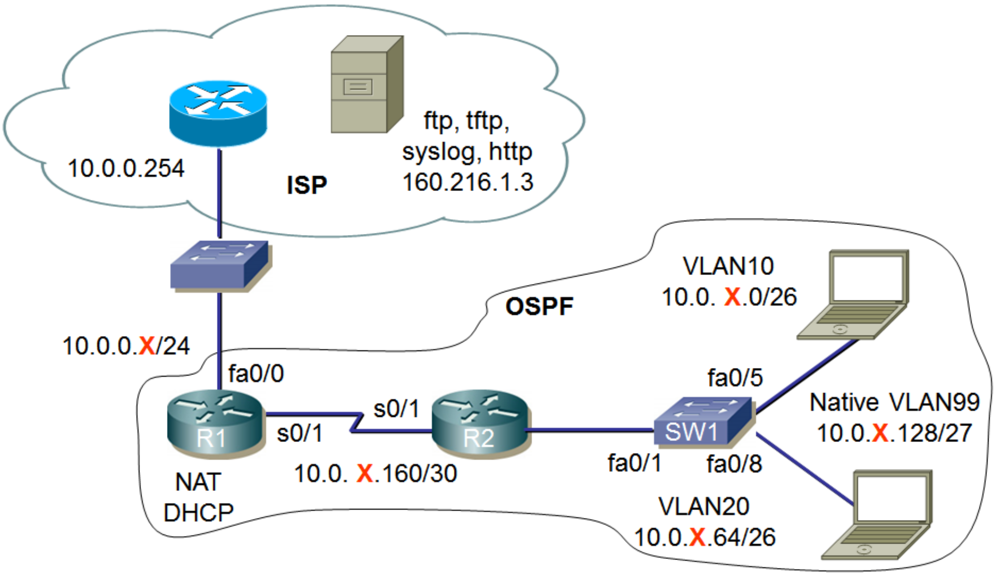
X=

CCNA 7 – ENSA, chapters 11, 12



Tasks:

1. Connect the network as shown in the diagram.
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. Create a VLAN on the switch, including a native VLAN (99).
5. For specific IP addresses, select the lowest possible for routers and the highest possible for stations.
6. The routing protocol will be OSPF, (it will propagate the default path information).
7. Network 10.0.0.0/24 will not be part of OSPF.
8. R1 router will perform address/port translation.
9. Router R1 will act as a DHCP server (DNS server is 8.8.8.8).
10. Set the ACL as follows
    - Allow access to the web server 160.216.1.3 for VLAN10 only.
    - Disable access to all other web servers for VLAN10
    - Disable access to the 160.216.1.3 web server for VLAN20 only.
    - Allow access to all other web servers for VLAN20
11. 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).

Guidelines:

1. First, connect the network, configure VLANs, IP addresses (write in this paper).
2. Then set up OSPF and verify functionality.
3. Set up DHCP server and verify functionality.
4. Finally, set up the ACLs.

Results

Write ACL

____

____

____

____

Write a command to verify the function (activity) of the ACL

____

____

____

Write a command to verify DHCP functionality

____

____

Results check

Basic setting

Passwords - R1 □
Passwords - R2 □
Passwords - SW1 □

Trivial service blocking □
VLAN □
OSPF □
Remote computer access □

ACL

Access to the local web server from VLAN 10 is possible □
Access to any remote web server is not possible □
Access to the local web server from VLAN 20 is not possible □
Access to any remote web server is possible □

DHCP □
Files stored on the TFTP server □