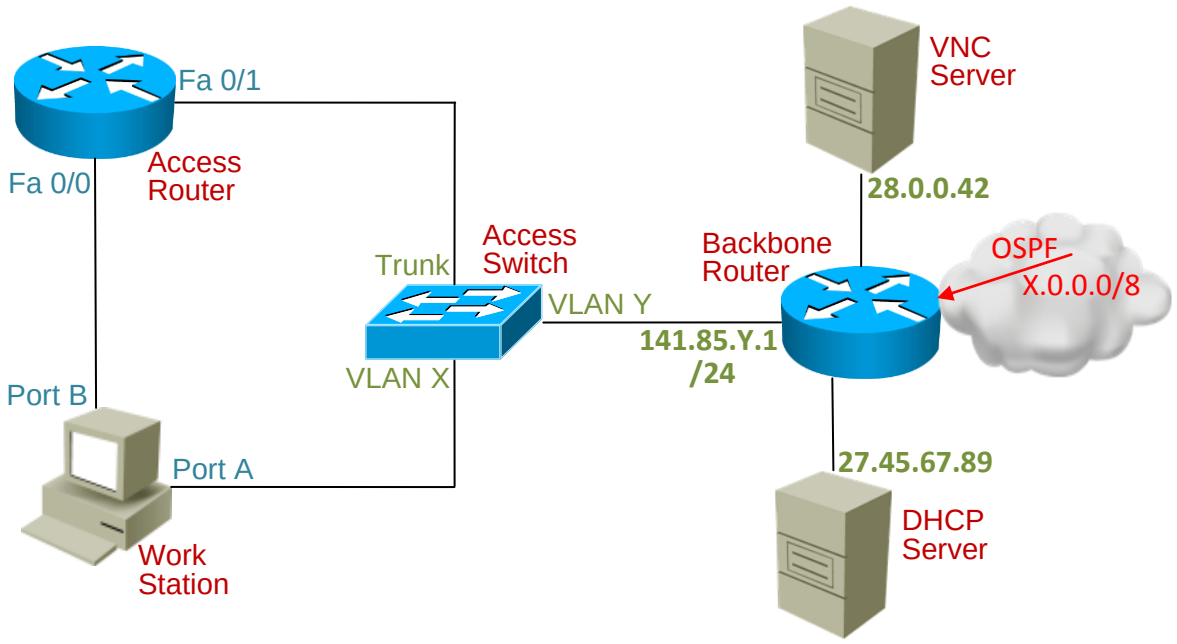
Topology:



The Goal:

Connect to the VNC Server (28.0.0.42) using the Tight VNC client on your workstation. Mark your access on the host by leaving your name in the Hackme.txt file (don't delete previous entries) on the Desktop.

The Story:

In order to prove your networking skills you have chosen to "hack" into a server from a different department from your company. The following information has been gathered for the devices represented above:

Topology information:

- **Workstation:**

The network cable from your workstations network adapter can be connected to:

- **Port A** (left port):
  - connected to the Access Switch on an **access port** from VLAN X, an undocumented VLAN.
- **Port B** (right port):
  - connected to the Access Router on **port Fa0/0**.

All Rights Reserved © 2011 CATC Romania

- **Access Router:**
  - **Telnet information** to this device: username "**instructor**", password "**cisco**". This account has limited access (only some commands are allowed).
  - **Interface Fa0/0** is configured, but the **IP address** and **subnet mask** are *not* documented. Also, incoming traffic to interface Fa0/0 has been **restricted**, permitting only traffic destined to the Router.
  - **Interface Fa0/1** is connected to a trunk interface on the Access Switch; this interface is not configured.
- **Access Switch:**
  - connected through an **access port** from VLAN X to port A
  - connected through an **access port** from VLAN Y, **Y=X+1** to the Backbone Router. The IP address of the Backbone Routers interface is **141.85.Y.1** from a **/24** network.
  - connected through a **trunk port** to the **Fa0/1** interface of the Access Router. The trunk port allows traffic from the two VLANs, X and Y.
- **Backbone Router:**
  - connected through a FastEthernet interface with the IP address **141.85.Y.1/24** to the Access Switch on an **access port** from VLAN Y
  - running two unsecured routing protocols using their **default administrative distances**. Only the following are known:
    - **OSPF** - the network X.0.0.0/8 is learned from the cloud through OSPF
    - **EIGRP** - the network 141.85.Y.0/24 is advertised through EIGRP, **Autonomous System Y**
- **DHCP Server:**
  - IP address **27.45.67.89**
  - directly connected to the Backbone Router
  - has as **default gateway** the IP of the Backbone Router interface
  - has a manual binding that allows the allocation of the IP address **X.C.D.E** in the **X.0.0.0/8** network to the hardware address **aa:aa:aa:aa:aa:aa**
  - the IP **X.252.253.254** is excluded from any pool on the DHCP server and it is assigned as **default-gateway** for the X.0.0.0/8 network
- **Access Server:**
  - IP address **28.0.0.42**
  - can only be accessed from the IP address **X.C.D.E** in the **X.0.0.0/8** network
  - directly connected to the Backbone Router
  - has as **default gateway** the IP of the Backbone Routers interface

All Rights Reserved © 2011 CATC Romania

Restrictions and Hints:

Useable applications on workstation:

- **Wireshark** – a protocol analyzer application
- **Putty** – a terminal emulator application which can act as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols and as a serial console client
- **Command Prompt** – the Microsoft-supplied command-line interpreter on Windows NT-based operating systems
- **Tight VNC Client** – Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer.

There are no *other* traffic restrictions previously configured through the topology.

1) Using the available applications determine for port A the corresponding VLAN on the Access Switch (**VLAN X**)

2) Determine the **IP address of Fa0/0** on the Access Router and configure accordingly IP addressing on the network adapter of your workstation.

3) **Telnet** to the Access Router through Port B and configure the Access Router so that the traffic from port A can be forwarded to the Backbone Router interface.

   Considering the access limitations for the VNC Server, your goal now becomes the assignment of the IP X.C.D.E from the X.0.0.0/8 DHCP pool to your workstation. Keep in mind how the DHCP server assigns IP addresses when allocating the IP for the VLAN X subinterface.

4) Configure end-to-end connectivity between your X.0.0.0/8 network and the other devices in the topology.

   Traffic from your workstation must reach the Access Router, the Backbone Router, the DHCP Server and the VNC Server. At this step, keep in mind the routing tables from all of these devices and how you can alter them to your advantage if necessary and/or possible.

5) Obtain the IP address **X.C.D.E** from the DHCP server through Port A and connect to the VNC Server using the client on your workstation.

All Rights Reserved © 2011 CATC Romania

Useful tutorials:

➢ Wireshark basic guide:

Wireshark is a protocol analyzer based on *pcap libraries* commonly used as a diagnostic tool for network and network application development. Frames received on a network adapter can be therefore captured and analyzed.

Start a capture by opening the Capture interfaces menu – click on the **icon shortcut** or on the menu bar: **Capture -> Interfaces** and then click **Start** on the Intel Interface Adapter.

The output of the captured packets can be filtered by typing key words in the **Filter field** just above the packet output.

Inspect a targeted packet by selecting it in the packet output.

➢ Command Prompt – how to start and useful commands:

How to start Command Prompt: click **Start -> Run** and type **cmd.**

Useful commands:

- **ipconfig** and **ipconfig/all** – display basic and detailed information of the addresses used by the local network adapters
- **ping** – test Layer 3 connectivity using ICMP packets
- **tracert** – display hop-by-hop connectivity with a target IP address

➢ How to change the IP address in Win XP:

Steps:

- Navigate to **Control Panel** (Classic View) > **Network Connections**
- Select and **right click** on the targeted network connection, and then click **Properties**
- In the **General tab** of the window that will open, click once the **Internet Protocol (TCP/IP)** item, and click **Properties**
- The Internet Protocol (TCP/IP) Properties window will open. In the **General tab**, click for:
  - A manually configured static IP address -> **Use the following IP address**, and enter the IP address, Subnet mask and if needed, the Default gateway
  - An IP obtained through DHCP -> **Obtain an IP address automatically**
- Click OK in all the previously opened windows.

All Rights Reserved © 2011 CATC Romania

- How to change the MAC address of a network adapter in Win XP

Make sure to close Wireshark before changing the MAC of your network adapter.

Steps:

- Navigate to **Control Panel** (Classic View) > **Network Connections**
- Select and **right click** on the targeted network connection, and then click **Properties**
- In the **General tab** of the window that will open, click the **Configure** button next to the network adapters name
- Select the **Advanced tab** of the window that will open, select **Locally administered address** and enter the custom 12-digit hexadecimal number (Custom MAC ID) ranging between 0000 0000 0001 – FEFF FFFF FFFF (without spaces)
- Click OK in **all** the previously opened windows.

*In order to display the currently used MAC addresses, go to your **Command Prompt** and enter the command **ipconfig /all**.*

All Rights Reserved © 2011 CATC Romania