Chalmers University of Technology

Department of Computer Science and Engineering

Computer Communications

Network Address Configuration

COMPUTER COMMUNICATIONS

Network Address Configuration

Chalmers University of Technology
Department of Computer Science and Engineering
Division of Networks and Systems

CONTENTS

1. Purpose

In this assignment you will build a sub-network and configure a number of PCs to work on that network. You would also be connecting your sub-network to the other group's sub-networks and send network traffic between them.

2. Overview

The assignment should be performed according to the procedures outlined below with the use of equipment in the lab. The following tasks will be performed:

- Construction of a local area network (LAN) and configuration of Windows hosts
- Running a number of commands to verify and diagnose the network
- Building a larger network with other groups, IP Subnetting
- Use of Wireshark (or Observer) to monitor local traffic

3. Preparation at home

The following tasks should be performed at home before the lab and a written report must be given to the teachers in the lab. Note that there is not enough time in the lab to do the preparatory work at that time!

1. Read chapter 4.4.2 (page 342-356) in the book about IP addressing. In the lab, we will create a Class C network, i.e. a network with a 24-bit subnet address and an 8-bit host part (aaa.bbb.ccc.ddd/24). Answer problem 11 on page 422!

2. Read chapter 5.6 (page 480-487) about switches.

3. Read chapter 5.4.2 about the address resolution protocol (ARP). What does it do? Why is it important?

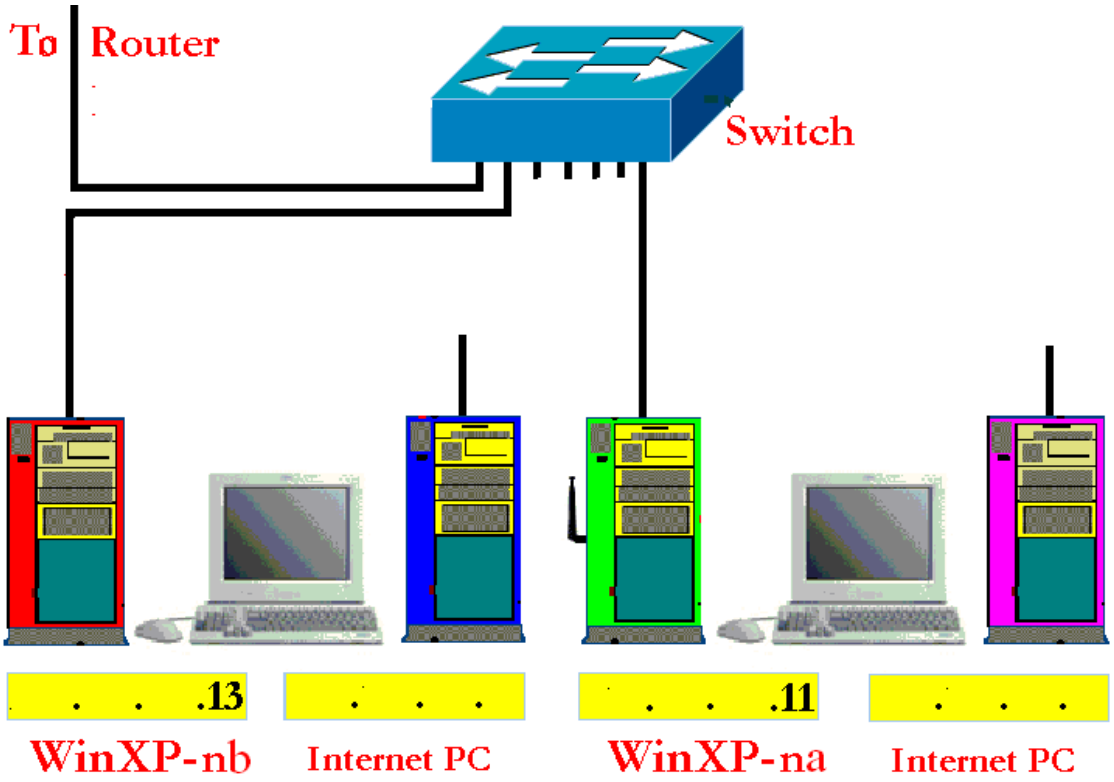
4. Investigate the following commands that can be used for diagnosing a network: arp, ping, ipconfig and tracert. What do they do? Try to explain their functionality in words such that another person who has never seen the commands can understand what they do and why/when he/she would use it.
Run the commands on a Windows system (on Unix/Linux systems, tracert is called traceroute) until you become familiar with them.

Hint: More information about the commands can be obtained on Windows by hitting "F1" (help) on the desktop and by typing "arp /?" in a command window.

On Unix/Linux systems, more information can be obtained from the on-line manuals: "man arp". Include some examples of output from these commands in your report and explain the resulting output!

4. IP Subnetting

You will be working with equipment in a closed environment where the equipment has no connection to the external world. The figure below shows the equipment at every workplace in the laboratory.



Exercise 1: Find out what IP address your two Windows computers have using the <ipconfig /all> command, for example. Your computers are connected in a peer-to-peer LAN configuration.

IP address: **and**

Network mask: **and**

What is the decimal and binary representation of your computer's IP address?

Decimal:

Binary:

What parts of the IP address represent the network and respectively the host part of the IP address?

Network:

Host:

What is the default gateway, and the computer's physical address?

Gateway Address

Physical Address:

Check how your Windows system routes packets. Use the <route print> command. What information do you get? Try to analyze the output and write relevant information here:

Exercise 2: Execute the command <arp -a>. Ping your neighbour's computer in your own group and run the command again. Then ping another group's computer. Run <arp -a> again.

Assume hypothetically that you are given an address subspace. The local network in the lab will have the address 200.150.100.0/24. We will divide this subspace (200.150.100.0/24) into subnets, i.e. to create one subnet for each group (or one per table). What is the class for the network address 200.150.100.0/24?

Now assign a new IP address to your computer. Your computer's new address should be 200.150.100.x where x is replaced by the last three digits on the computer's red label. (Example: the label P01-40 means x=140.)

New IP Address:

The address can be changed from "Network Connections" which you can find in the control panel. Click on "Network Connections" and select the icon "Peer-to-peer LAN" for your local area network, right-click on it and select "properties". Now you can see a number of properties for this connection. Select "Internet Protocol TCP/IP" and look at the parameters you can configure.

Change the computer configuration to use the new address! Also look at the other TCP/IP parameters that are possible to change (but leave them as they are) and try to explain them.

After changing your computer's IP address, ping your neighbour's computer in your own group and run the command <arp -a> again. Then ping another group's computer and run the command <arp -a> again. Explain why computers in your vicinity as seen by your computer have changed.

Why doesn't the router forward the packets as before?

Exercise 3: Now we will connect your network to other groups' network to form one single IP network for all computers in the lab and make sure that all computers can communicate. (You have changed the IP address of your computer; specifically both the network part and host part which results in that the network part of the computer's IP address differs from that of the router interface's IP address.)

Begin with making sure that all switches in the panel are connected to each other.

Switches are marked with "switch-1, 2, 3, and so on. Switch 1 will be used for the first subnet, switch 2 for the second, etc. Connect your switch with another group's switch (1_ 2, 2_ 3, 3_4, and so on using crossover cables. Test the network and make sure it works!

Ping another group's computer. Then run the command <arp -a> again. Explain what has happened when the switches are connected. Note that currently there is no default gateway. All computers are now connected and form one large IP network.

What would be the purpose of adding a default gateway to the network?

Click on the icon on your desktop "My Network Places" to see the groups/computers connected to you. (Microsoft has its own protocol that allows Windows computers to announce their presence to other computers by sending broadcast messages on the network. The result from these announcements can be seen under My Network Places but it can take some time for this to update.).

What groups/computers do you see?

Exercise 4: Now the single IP network will be reconfigured into a number of subnets. You will now change the IP address of your computer, making the network part of your network different from all other groups. We will use the network 200.150.100.0/24 for this exercise and divide it into subnets. What does it mean when an IP address has the host-part as all zeroes, i.e. 200.150.100.0/24?

What does it mean when an IP address has the host-part as all ones, i.e. 200.150.100.255/24?

Assume that we will create 8 subnets out of the larger IP network. This is sufficient for connecting each group's computers together and still leaves plenty of room for computers within each subnet.

How many bits will be used for the network (subnet mask)? ----------

How many bits will be used for the host-part in each subnet? ----------

Complete the following table that shows the details for each subnet:

SN#	Subnet Address	Host IP Addresses	Broadcast Address
1	**200.150.100.0**	**200.150.100.01 Up to 200.150.100.30**	**200.150.100.31**
2			
3			
4			
5			
6			
7			
8			

Exercise 5: We will now perform a logical separation of the subnets. Group 1 should use subnet 1. Group 2 should use subnet 2, etc. Leave the first available address for the router interface connected to your network, i.e. for the default gateway. One computer should use the second IP address in the subnet and the other use the last IP address in the subnet.

My subnet: **Network mask:**

Select valid IP addresses for your computers.

Computer 1:

Computer 2:

Default Gateway:

Configure your computers for these IP addresses. Make sure to configure with the new network mask!

Start the program Observer (or Wireshark) to see the network traffic:

Send a ping command from your computer 1 to computer 2. What happens?

Try to find the IP addresses of all computers on the network using Observer's "Discover Network Names" function or using Wireshark. (If using Observer, select <Use Time Limited Function Demo> after you start the application. Then select Tools_Discover Network Names and press the green start button.) Observer will show all MAC addresses in a table. With Ethereal you have to search for them in the collected data.

Collect some statistics about network usage with the "Statistics _ Pairs Statistics (Matrix)" command in Observer. This command displays graphically all interfaces the application (Observer) has seen on the network and draws a line between pairs of interfaces that it has seen communicating. Why do you not see traffic between the other group's computers?

Discuss the advantages and disadvantages of using this kind of logical grouping of hosts by subnetting although hosts are physically still connected using switches on the network.

What will be needed to allow communication between hosts belonging to different subnets?

What is the difference from using physically separate LANs/subnets instead?

Exercise 6:
Restore the computers' IP addresses to the original addresses as they were before you changed them. Use the same configuration as when you came into the classroom, using the original default gateway, subnet mask. Remove the crossover cables from the switch.

5. Routing and Router Configuration

Router configuration is outside the scope of this course, but we will now look at how the router is configured. The router is configured to be your default gateway and receives all traffic from your network that is destined for other networks.

Exercise 1: You can telnet to the default gateway (router's interface) of your LAN to see the router's configuration. Start Telnet (in a command window) to connect to your router. The address of your router's interface for your LAN is the address of the default gateway (and can also be found in the network diagram on the desk).

The first password is "cisco". After successful authentication you are in user mode where some of the router settings can be checked. To configure the router, another login is required using the "enable" command and the password "class". Now you are working in privileged mode and configuration is possible. NOTE: for more information about privileged mode and before doing any router configuration, contact the Lab instructors!

If an error is made when configuring the router, it may not be possible to talk to it over the network anymore. Therefore, the router has a console interface (with a dedicated serial communication cable), which is always possible to use. You can test this if you want. Click on the icon on one of the Windows PC desktop named "Console Router n" (where n is the number of your group) to open a Windows "Hyper Terminal" to communicate with the router in console mode.

We will now investigate two router commands: "show run" and "show ip route".

Exercise 2: Execute the command <show run>. Try to figure out the output. Which router interface belongs to your network and what IP address does the interface have? Ask your lab instructor regarding how to interpret the output.

What routing protocol is configured and for what networks?

Run the command <show ip route>. With whom do you have directly contact with? Select another group's LAN and determine the route to that LAN from the routing table. How many hops away is the LAN according to the routing table? (Cisco routers show the metrics using [120/x] notation where x is the cost or hop count.). Compare the number of hops to what you would get by examining the network map. Are they equal?

Run the command <tracert> from your computer to a computer in another group. Look at the network map. How many hops do you get? How does this compare to the distance metric provided by the router when you run <show ip route>?

Exercise 3: Start Wireshark by clicking on the Wireshark icon on your desktop. Run the command <tracert> to a computer in another group again and answering the following questions.

What types of protocols can you see on the network? What protocol is used when you run <tracert>?

Do a <ping> of the same computer. What protocol is now used? The ping command accepts as an argument the size of the (dummy) data to send: <ping –l size computer>.

Experiment with some sizes and observe the size of the packets on the network using Wireshark. What is the default data size when using ping? How much is the overhead (compare with the amount of data being sent over the Ethernet cable)?

Capture packets by Wireshark and filter to display only RIP-packets. What destination IP address is used for the RIP messages sent by your router on your LAN? Examine the different parts of the packet header.

Examine the different parts of the RIP message itself. What RIP version is used? What routing information is included in RIP message?
