Laboratory Week 11 – Configuring Wireless Networking

Aims:

- To configure a small home/business network for dual wired/wireless access
- TO configure a small home/business network to access the Internet

Background:

Wireless Access

Wireless is just another Link-Layer technology. It is often called Wireless Ethernet because the layer 2 frame format is the same as the Ethernet Frame Format. However, the actual link layer protocol behaves differently to the Ethernet Link Layer protocol. In some advanced configurations, you may be able to tweak portions of the Wireless Link Layer behavior, however in almost all actual deployments the default Wireless protocol is used to manage a wireless network.

Wireless Access Methods

Wireless connectivity can be provided in Ad-Hoc mode or Infrastructure mode.

1. **Ad-Hoc Mode** allows each device on the network to freely communicate with any other device in Ad-Hoc mode, there is no controlling infrastructure to moderate access to the wireless domain. In Ad-Hoc mode, there are a number of issues with regards to hidden-nodes which are not addressed, further communication may involve the deployment of peer-to-peer routing between all wireless nodes to move traffic across the network. Ad-Hoc mode is rarely deployed on consumer or access devices, however it is regularly used in widespread sensor networks and in networks where nodes are continually moving such as the newly proposed Vehicle-to-Vehicle networking technologies
2. **Infrastructure Mode** is one where a central Access Point moderates access to a network for all mobile nodes in its domain. As well as dealing with any possible hidden-node problems, it also provides a simplified architecture in that all mobile nodes communicate with the Access Point only. Data destined to other mobile nodes must still pass through the Access Point, even if those mobile nodes could communicate with each other. Infrastructure mode also allows for simplified access to non-wireless networks. By connecting the Access Point to the Internet in general, the Access Point becomes a “gateway” for all wireless devices to communicate beyond the wireless domain and to the Internet. By having this single point, network design is simplified as there is single connection point between the wired network and the wireless domain

Network Layer Connectivity

The aspects of moving between link layer technologies are hidden through the use of the IP protocol. This allows us to easily move between domains without changing the protocol we use for communications.

There are three basic approaches to deployment of wireless access in networks, the first two involve networks that only have a single access point and you need to decide whether to share the subnet between wireless and wired infrastructure (single link-layer network) or to separate the two technologies into different subnets (unique link-layer networks). If multiple access points are required, we are typically considering a larger deployment that will involve the use of managed switches and VLANs. In this case we often allocate a single VLAN to all wireless networks and link all the Access Points into a single VLAN, sharing the link layer network between wireless and the wired connections between the Access Points. While it is possible to deploy multiple access points with a unique subnet for each access point, this is not a common deployment strategy.

1. **Simple Single Layer Network.** To share a wired network and wireless network in the same link layer network, we need to configure our Wireless Access Point in bridging mode. In this case, the Access Point behaves as a switch where some of the switched ports are physical Ethernet interfaces. The actual wireless point becomes one port on the switch. Despite the fact that both link-layer technologies are different, they appear to be a single link layer to the network. On cheaper wireless routers where there are usually approximately four LAN ports on the back of the device, these ports are all switched with the Wireless node and both wired and wireless devices can share the same subnet/link-layer. For small networks where segregating wired and wireless traffic is not

important (such as you home network or a very small business), this can be an attractive choice due to ease of configuration of not only the wireless, but of any other service configured on the network.

2. **Unique Link Layer Networks.** The Wireless Access point typically acts as a router segregating the wired and wireless portions of the network. As the two networks now operate on different link layers, they need to be linked by a router. For small networks where you care about segregating wireless and wired traffic, this is a very common solution and is regularly deployed in small businesses that only have a single Access Point. The deployment comes with the added complexity of managing a new subnet and having to ensure that services are available across both subnets.
3. **Multiple Access Points.** The Access Points are typically configured in bridging mode and bridged onto a dedicated VLAN within the switched network. Traffic between the wireless and wired domains is segregated by virtue of the VLAN arrangement and routing is performed by inter-VLAN routing in your wired network. Having a common VLAN for the wireless domain simplifies configuration and allows users to move between wireless Access Points without losing connectivity to the network. This deployment is very common across larger corporations with multiple access points. It is much preferred to deploying Access Points as routers to minimize issues with users roaming across access points and to simplify deployment of security protocols.

In this lab we will be deploying Option 1 above, mainly to give you some experience with configuring a Wireless Access Point for a small business environment, but also because the Cisco-based wireless equipment at CCNA level is predominately a simple wireless router based solution. Our switched network will be simulating the network (using subnet 192.168.100.0/26) which the LAN side of the Wireless Access Point will be acting as the company network (using subnet 192.168.200.0/24)

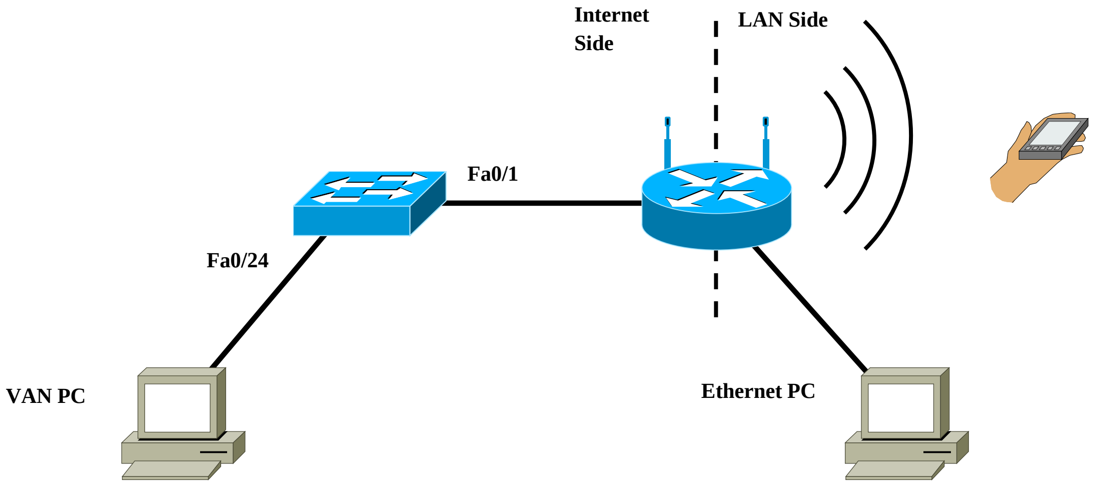
Methodology:

Reserving equipment

Please book a whole kit for this lab, however we will only be using a single switch in it's default configuration, all configurations will be done on the Wireless Router. Your Lab Supervisor will open the cupboard containing the Wireless equipment.

Physical Network Configuration

Please book a whole kit for this lab, however we will only be using a single switch in it's default configuration, all configurations will be done on the Wireless Router. Your Lab Supervisor will open the cupboard containing the Wireless equipment.



Setting up the Wired Switched Network

We will not be performing any configuration on our Cisco Switch. You just need to confirm that the switch is clean (no saved **startup-config** or any saved **vlans**) prior to continuing with the lab.

We will be deploying the subnet **192.168.100.0/26** on the wired side of the network. Configure your VAN PC with a host address in this subnet with the appropriate subnet mask. Configure a default gateway on the VAN PC of **192.168.100.1** (don't use **192.168.100.1** as an IP address for a PC).

The VAN PC will be acting as an Internet based PC for us to connect to with our company computer later.

Setting up the Wireless Router – Basic

To help with the router configuration, this document will refer you to the **Wireless_7_5_1_Instructions.pdf** file available on Blackboard. This file is the old ***Cisco CCNA3 Wireless lab handout*** but more importantly includes specific instructions on how to perform tasks when configuring the Wireless router.

NOTE: Your wireless router will be configured at your desk using the Ethernet Virtual PC. Please complete Task 2 from the **Wireless_7_5_1_Instructions** handout to clean the wireless router and to access it for configuration purposes.

NOTE: TO configure the network, the patch lead that is usually plugged into the patch panel at your desk to go to your rack should now be plugged into a LAN port on your router. When you are ready to connect your router to the Internet, you should obtain a patch lead and connect the Internet port of your Wireless Router to the patch panel on your desk and through to the switch in the rack.

The Ethernet PC will be a wired computer connected to your Company network.

Setting up the Wireless Router Basic Configuration

We will first configure the some basic network settings on the router such that it is using the correct IP addresses, and that wired devices in the company LAN will be able to access the Internet. We will configure wireless connectivity at a later stage

Complete Task 3 from **Wireless_7_5_1_Instructions** to configure the router using:

Internet IP:	192.168.100.1
Internet IP Subnet Mask:	/26
Default Gateway:	IP Address allocated to your VAN PC
Network IP Address:	192.168.200.1/24
DHCP Server:	Enabled

The Internet side of the router will connect to our wired network so it needs to have an IP address configured in that subnet. Typically, you could run a DHCP client on the router as most ISPs will allocate an IP address to their customers using DHCP. As you do not know how to configure DHCP on Cisco products, we will manually configure the Internet side of the link. The Wireless Router will also act as the Router for our VAN PC to communicate with the LAN side of the router. The Network side of the router will configure the wireless clients and the Ethernet PC connected to the LAN port. Enabling DHCP will ensure that our LAN clients (Ethernet PC and wireless hosts) will be automatically assigned IP address configuration (appropriate address/mask and to use the router as a gateway)

NOTE: The gateway address must be configured on the LinkSys Wireless routers. Given that we will not actually be traversing to a further network, the actual value typed in here is not important, you just need to type something to make the router happy. In a real-world scenario, the Internet IP/Mask/Gateway will typically be automatically assigned to your router by your ISP via DHCP

NOTE: The Ethernet PC will need to be detached and reconnected to the LAN port on the Router. As the Router has changed its IP network, the PC will need to acquire a new address. Once the new address has been acquired, you will need to configure the router via its new IP address (**192.168.200.1**)

You should now be able to test connectivity from your VAN PC to the wireless router, and from your Ethernet PC to both the Wireless router and VAN PC. The Wireless router will route traffic between the two subnets.

NOTE: You will not be able to ping from the VAN PC to the Ethernet PC because the router is implementing NAT between the LAN and Internet side. NAT allows multiple devices on the LAN side to share a single (real) IP Address when accessing the Internet, as packets leave the LAN side, the router will change the source IP address to the Internet IP address (and sometimes the source TCP/UDP port number). This is done because you don't own the addresses used on the LAN side and packets to these addresses from the Internet will not be delivered to you. The router will store the mappings in a NAT table. Return packets from the Internet are always addresses to the Internet IP address, when a reply packet comes, the router will correctly adjust the destination IP address (and possibly destination port number) from the Internet IP address to the internal LAN address using details from the NAT table. The upshot is that all connections must be established from within the LAN so the NAT table can be properly maintained, the router will not know how to correctly deliver a packet when the connection is established from the Internet side of the router. To summarise – your Ethernet PC (and later in this lab mobile devices) will be able to ping the VAN PC (in the Internet), but the VAN PC will not be able to ping your Ethernet PC or mobile devices.

NOTE: Do not continue until the Ethernet PC can ping the VAN PC.

Setting up Basic Wireless access on the Router

We will first configure wireless access for LAN clients. Note that we are not configuring any wireless security. It is often a good idea to confirm that your basic configuration is functional without security before deploying security features. This allows you to confirm that any problems reside with your security settings instead of elsewhere in the network.

Complete Task 4 from **Wireless_7_5_1_Instructions** to configure the router using:

SSID:	W<student_number>
Wireless security:	Disabled
Inbound ping requests:	Allow

You should now attempt to connect your mobile phone to your wireless access point. Search for an open-access Wireless Access point with an SSID that matches your student number. When you have found it, connect your phone to that network. Your phone should acquire an IP address in the **192.168.200.0/24** network, find this information on your phone and make a note in your lab journal.

NOTE: If you do not have a mobile phone with WiFi capabilities, ask your lab instructor which PCs in the lab have wireless cards and how to run/configure the Wireless Virtual Machine

You should now be able to test connectivity within your LAN by ensuring that your Ethernet PC can ping your mobile phone. If you have an app on your phone to enable you to run ping, you should also confirm that you can ping your VAN PC from your mobile phone *(remember – due to the NAT you will not be able to ping your phone from the VAN PC*)

NOTE: Do **not** continue until you are able to ping your phone from the Ethernet PC

Configuring Wireless Security

Now that we have network connectivity, it is time to secure the wireless link (otherwise everybody will be able to access the LAN **AND** listen to traffic between mobile nodes.

Redo Task 4 from **Wireless_7_5_1_Instructions** to configure the router using:

SSID:	S<student_number>
Wireless security:	WPA2 Personal
WPA Passphrase:	ccna_wireless

Change the SSID to indicate that you now have a secure connection. Your mobile phone will now de-associate itself from your wireless network and you will have to reconnect. Reconnect your phone to the new SSID. You will be required to enter the password before you can connect to your network.

Retest connectivity by pinging your phone from both PCs

If you have time

Your VAN PC should have some software on it called **tinyhttpd** or similar (if you can't find it ask your lab instructor). Start the software and observe where it says the server directory is.

Open the server directory on your VAN PC and create a text file called index.htm. Populate this file with some simple HTML code to display a welcome page and your name, then save the file to disk.

- From your Ethernet PC, open a web browser and browse to the IP address of the VAN PC and confirm that you can access the website from your company wired PC.
- From your mobile phone, start the browser and enter the IP address of the VAN PC and confirm that you access the website from your phone.

Cleaning Up

If you have finished, you should re-do the reset procedure to clear your wireless router configuration before returning it to the cupboard. Also don't forget to unplug all cables and return them to their locations, and to release the switches you booked from the web site and confirm that the devices have been turned off in the enclosure