For the last several years, I've worked with a group of world's best communications engineers.

I been continually been consulted on questions about how to set up home or small enterprise networks. If these people, who are among the most knowledgeable when it comes to the technology behind communications and networks, need guidance, I can imagine that the average person could use some practical information about how to set up a network for their home or business.

This series of slides is intended to provide an overview of how such a network might be configured.

Every network is different – this example is used for illustration purposes only. For specific designs for your network, please refer to the contact information on the top level page for this site

Angus
314.15.19.3

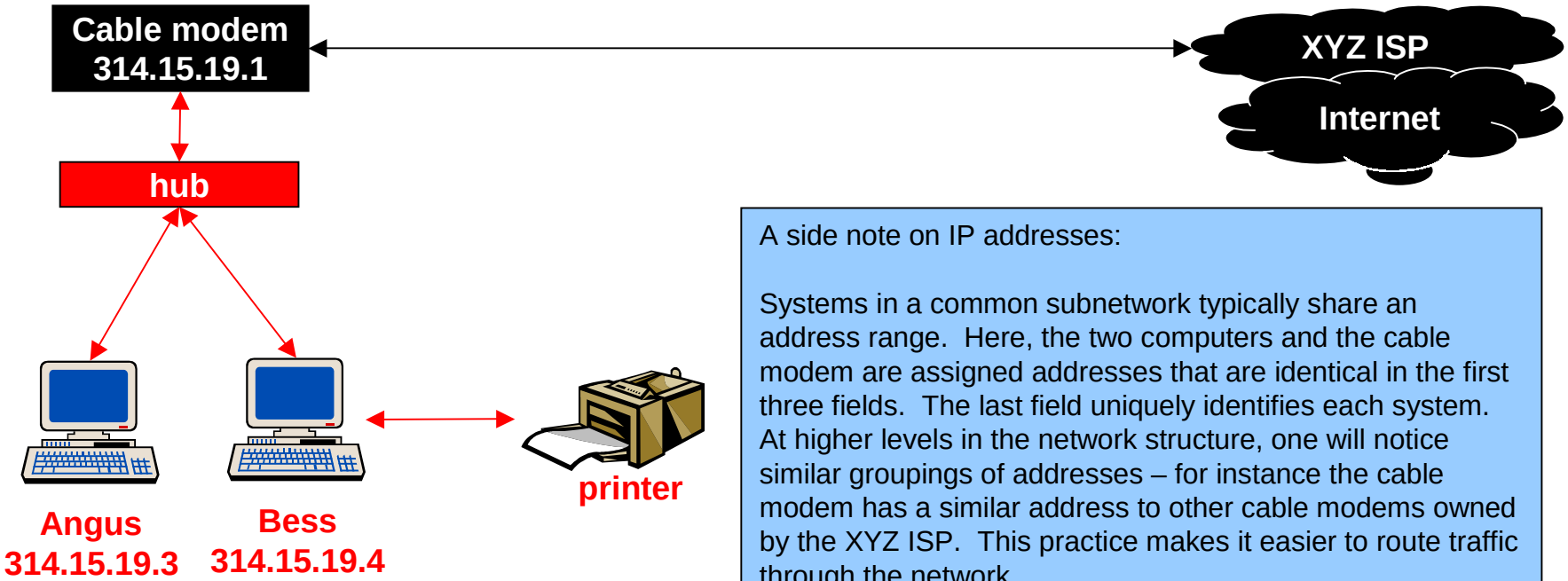
Let's start with the simplest network. (I'll be building up to something resembling my home network as a example. Some of the IP addresses have been made intentionally fictitious to avoid confusion with actual IP addresses.)

We are using the XYZ cable internet service. It could just as well be DSL – our home network would look about the same.

The cable modem is the interface between the access network and the home network. Here, there is only one PC (angus) behind the cable modem.

Other than the exposure of angus to the evildoers on the Internet, this network is pretty simple. To illustrate security on this network, I'll use standard security terminology – the **RED** portions of the network are those containing sensitive information that must be protected. The **BLACK** portions of the network are assumed to be under the control of the bad guy.

This network has some potentially serious problems – there is nothing separating the red and black sections of the network.

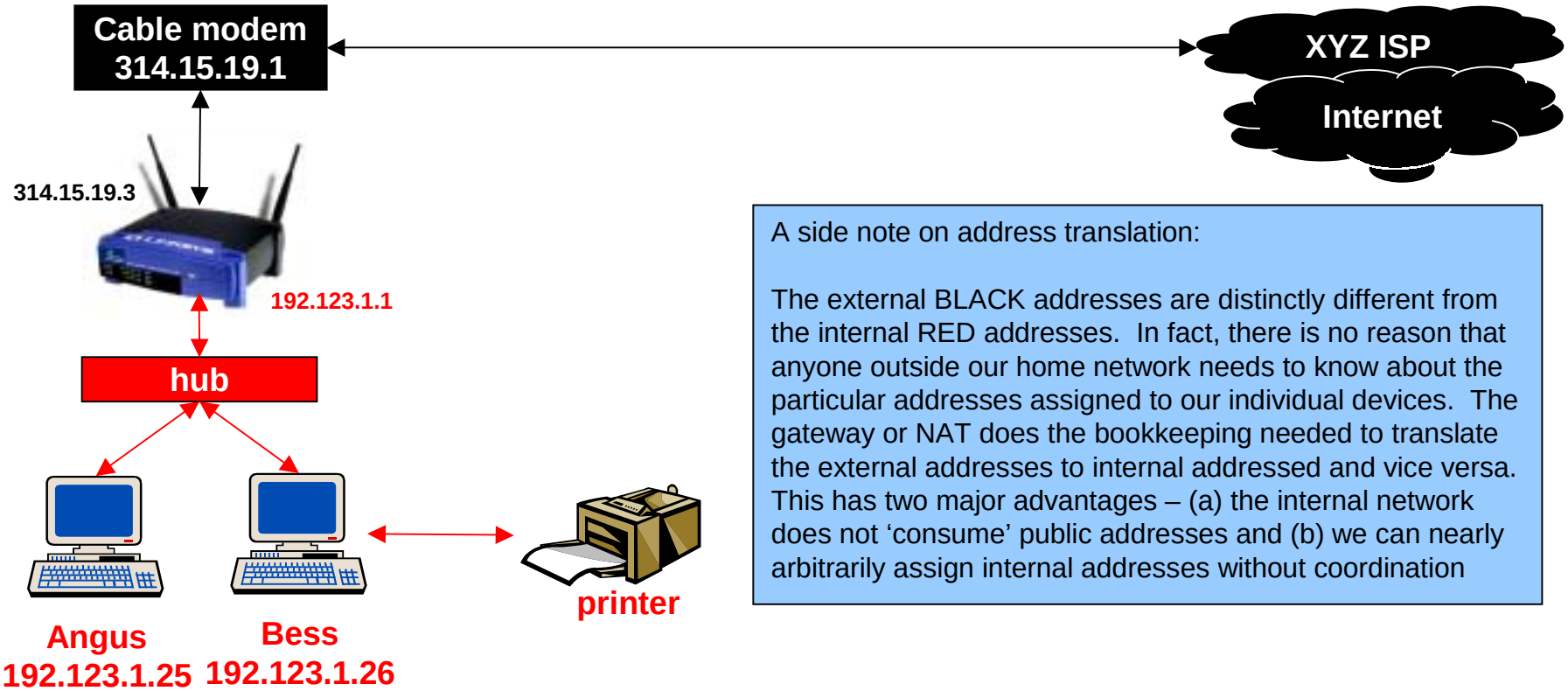


A side note on IP addresses:

Systems in a common subnetwork typically share an address range. Here, the two computers and the cable modem are assigned addresses that are identical in the first three fields. The last field uniquely identifies each system. At higher levels in the network structure, one will notice similar groupings of addresses – for instance the cable modem has a similar address to other cable modems owned by the XYZ ISP. This practice makes it easier to route traffic through the network

Now let's add some things to make the network a little more interesting. Assuming the ISP provides for multiple IP addresses, we can connect two or more PCs to the network.

Most likely, we may have a printer connected to one of the PCs. Very likely, it may be desirable to be able to share the printer with all the PCs on the network. Once the network is set up for print sharing, PC to PC file sharing is probably not far behind. This is where the red/black separation becomes an issue. For all practical purposes, the home Ethernet (all the wiring behind the cable modem) should be assumed to be completely open to the wild Internet.

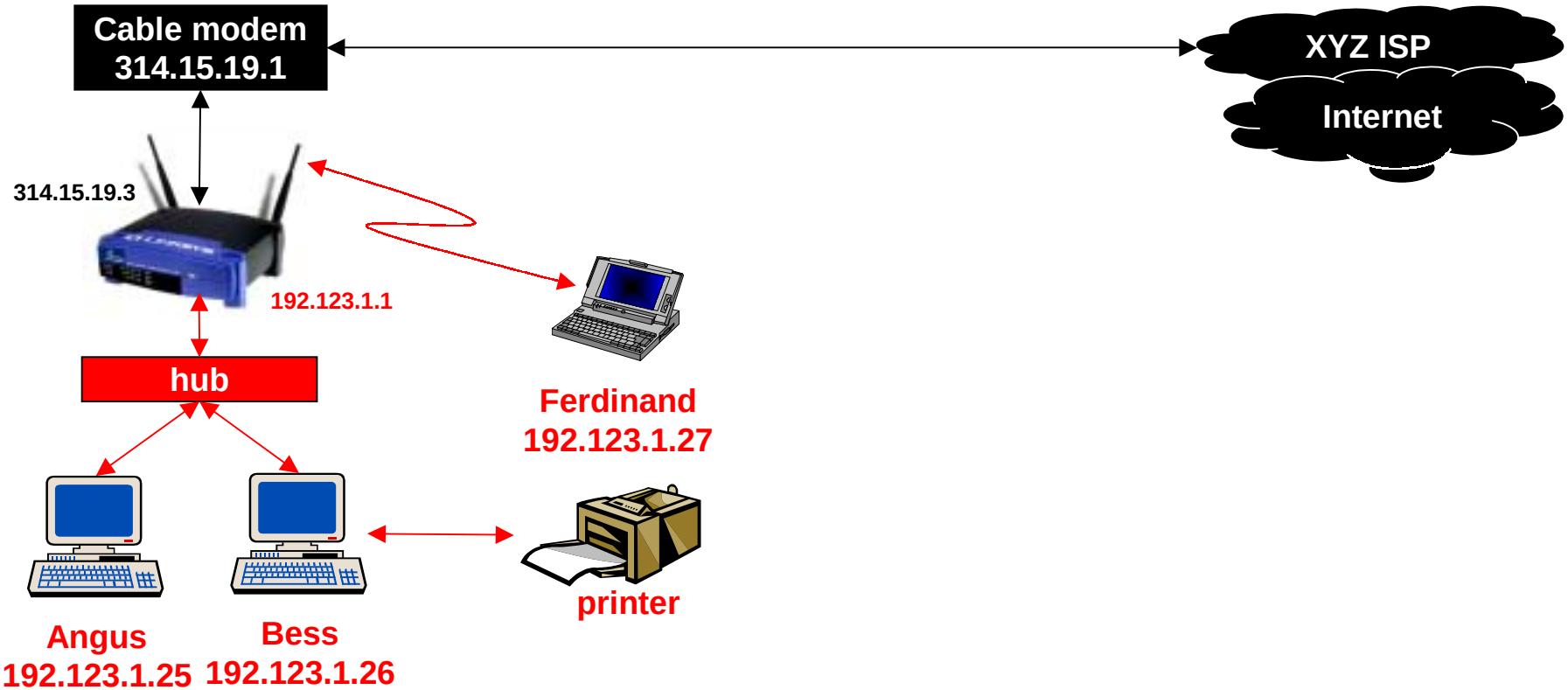


A side note on address translation:

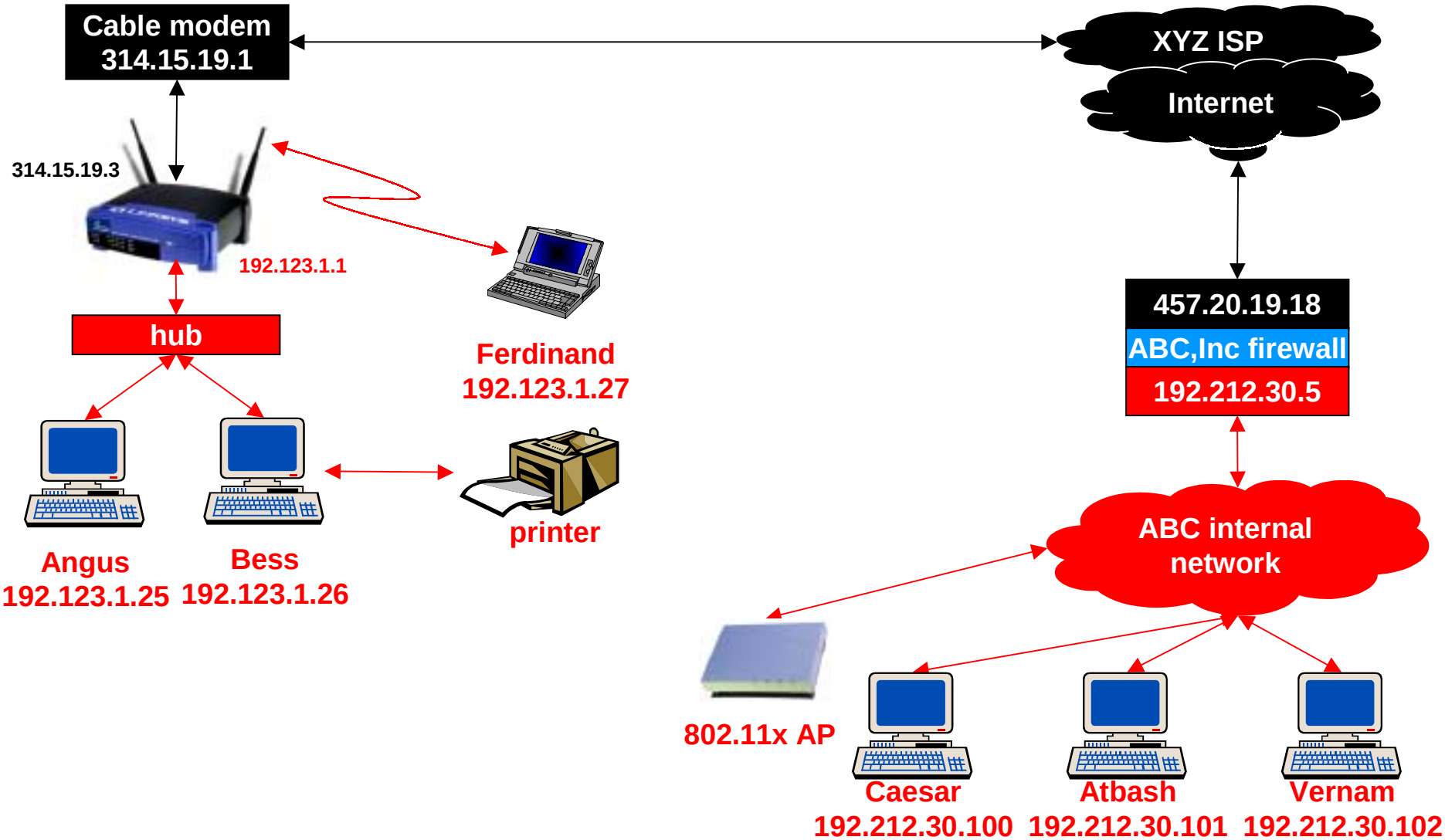
The external BLACK addresses are distinctly different from the internal RED addresses. In fact, there is no reason that anyone outside our home network needs to know about the particular addresses assigned to our individual devices. The gateway or NAT does the bookkeeping needed to translate the external addresses to internal addressed and vice versa. This has two major advantages – (a) the internal network does not 'consume' public addresses and (b) we can nearly arbitrarily assign internal addresses without coordination

Let's add a new piece of hardware: a router, a.k.a. a NAT or a gateway. This one happens to be a Linksys box that includes a 802.11b access point, but there are other brands and other variations that would do the job. This one happens not to include the function of the hub, but there are many that do. Some even provide the interface for print sharing, but I'll include this separately for reasons that will be clear later.

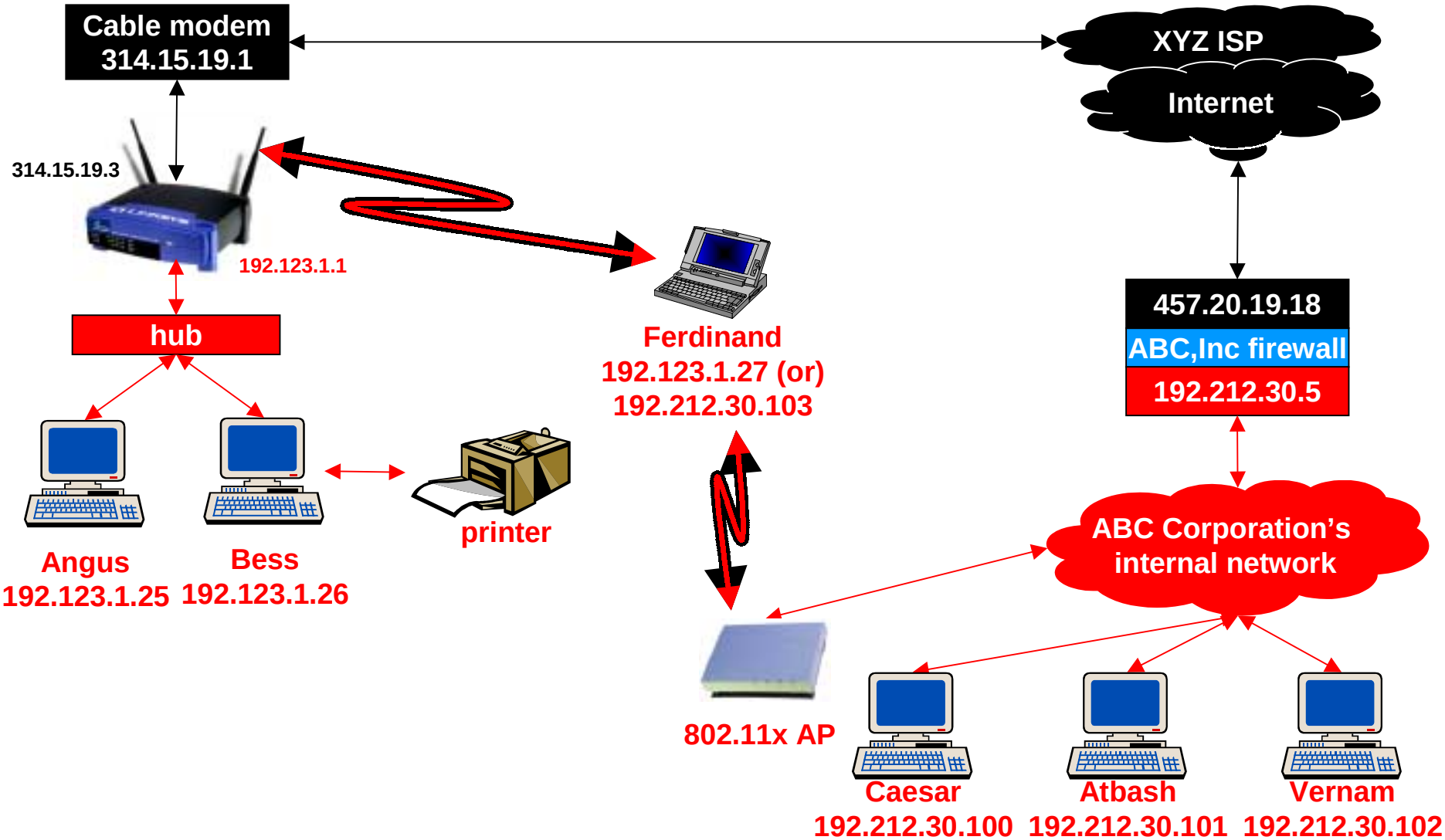
The addresses behind the router now bear no resemblance to those of the cable modem. That's because the Network Address Translator (NAT) function of the router has created a local numbering plan known and used only at our location. The router also provides red/black separation – we can block unwelcome traffic from the outside (evil) world.



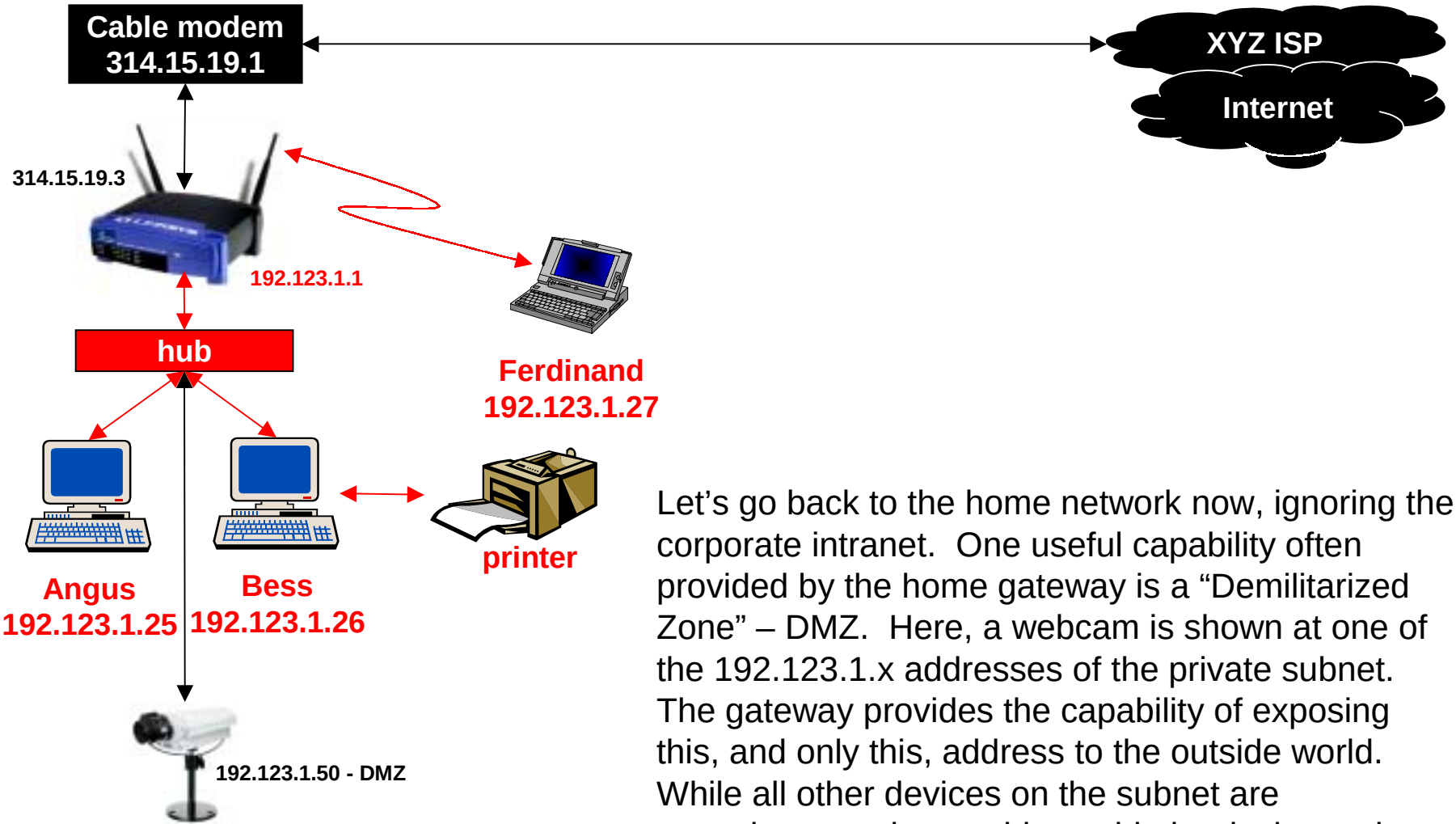
Before we really get complicated, let's add another computer: a notebook PC with an 802.11b wireless LAN card. This is going to be useful to illustrate extra features later when we start to move the notebook PC around the house and into the office at work. For now, suffice it to say that all the PCs are using DHCP (Dynamic Host Control Protocol) to obtain their IP addresses from the router. This really makes it much easier than trying to manually configure IP addresses across the network. Without DHCP, your chances of getting all the settings right without conflict is pretty small.



On the right side of the diagram, some of the internals of the ABC corporation are shown. They, too, have some hardware separating their internal network from the hostile Internet. They also use 802.11 wireless LANs in their buildings.

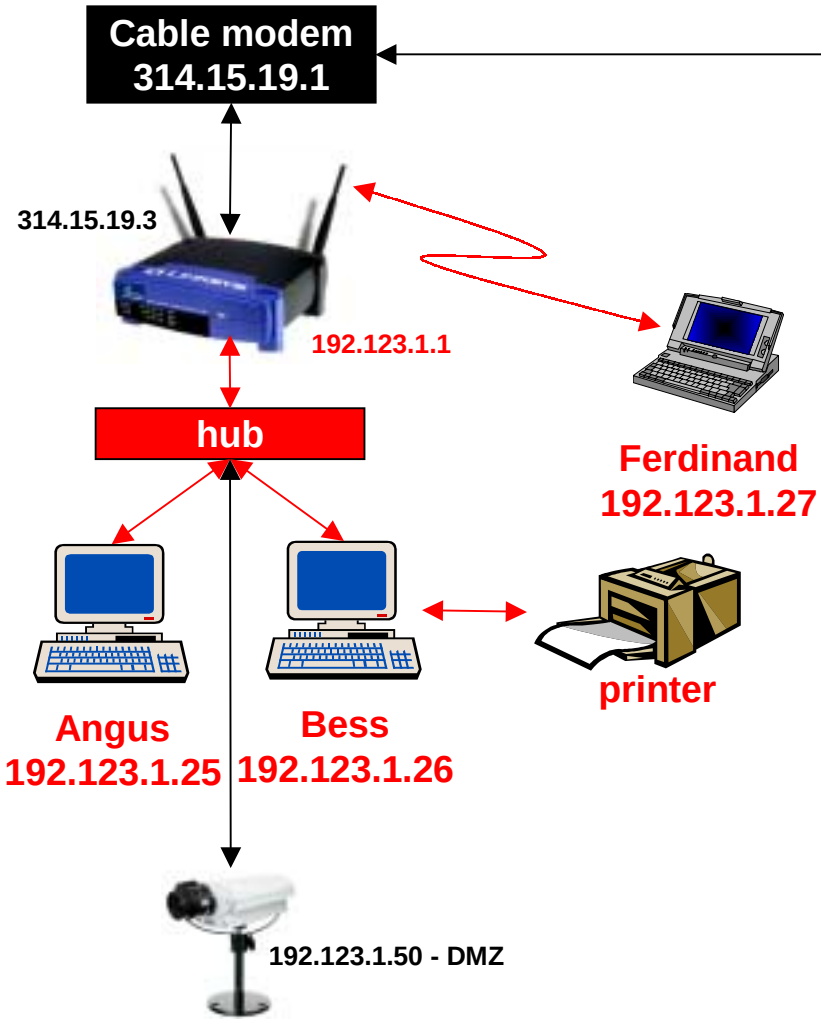


With appropriate Virtual Private Network (VPN) software (or hardware) to avoid the security vulnerabilities of the 802.11b Wireless Equivalent Privacy (WEP), the same laptop can be used at home or in the office, wrapping a sensitive (red) data path in an encrypted (black) VPN tunnel. With DHCP assigning the notebook's IP address, the PC works in either environment without the user needing to do anything as they work from the office or home.



Let's go back to the home network now, ignoring the corporate intranet. One useful capability often provided by the home gateway is a "Demilitarized Zone" – DMZ. Here, a webcam is shown at one of the 192.123.1.x addresses of the private subnet. The gateway provides the capability of exposing this, and only this, address to the outside world. While all other devices on the subnet are nonexistent to the outside world, the device at the DMZ address may be completely accessible.

Of course, you'd better be sure that the DMZ device can not be used as a backdoor into the rest of your network… In this case, the webcam is running a stripped down, minimal functionality version of embedded Linux and has no capability to access anything else on the 192.123.1.x subnet. The 192.123.1.50 address is translated to 314.15.19.3, so the webcam appears to the outside world to be the surrogate of the gateway itself.



Even for this simple network, there are a few simple security considerations worth noting:

- Many gateways support “MAC address cloning,” a simple way to hide the make and model of the gateway hardware – use it!
- Of course, you changed the default login and password for the gateway!
- Set all the router capabilities to the most secure state
- If you use a DMZ device, be sure it is does not create a gaping security hole
- If your gateway has an 802.11 AP built in, or if there is one on your subnetwork,
    - Filter wireless MAC addresses
    - Don’t announce your WLAN presence
    - Run WEP with the maximum available key size (it won’t stop a determined attacker, but there is no sense in giving this away)
    - Pick a secure key (‘sesame’ is a bad choice!)
    - Change the wireless network name to something unique and nonobvious
- Audit what the network is doing from time to time!