ICS 351: Today's plan

* IOS commands

* network monitoring

IOS modes

- the Internet Operating System (IOS) of the Cisco routers uses a command line interface, usually over a serial port
- IOS has a number of modes, each with a different set of commands:
- o user exec mode: ping, traceroute, telnet
- o privileged exec mode: can change configuration files, enter global configuration modes
- o global configuration mode: change system-wide configuration
- o interface configuration mode: change configuration of one interface
- o router configuration mode: change configuration of one routing protocol

IOS command-line interface

- different prompts in different modes
- question mark gives list of available commands
- some commands switch modes, e.g. enable enters privileged exec mode from user exec mode, disable returns to user exec mode
- in global configuration mode, ip routing enables IP routing, no ip routing disables IP routing
- in interface configuration mode, no shutdown enables the interface
- in privileged exec mode, show config displays the router's start-up configuration, show running-config displays the router's current configuration
- in privileged exec mode, reload sets the running configuration to the starting configuration, and copy running-config starting-config does the reverse

Network monitoring tools

- ping, telnet, ftp
- ping: find out if the other machine will respond
- telnet: find out if the server program will open a connection. Also, connect to a machine and enter commands remotely (but these days, more commonly done using ssh)
- ftp: transfer files to or from a remote system (but these days, more commonly done using scp)

Network monitoring tools

- tcpdump, wireshark (formerly known as ethereal)
- very similar in substance, very different in user interface
- configure the network interface(s) to listen to all packets: promiscuous mode. This is usually only allowed for the root user
- read all the packets on the network
- filter them (according to a packet filter) to only consider packets of interest
- parse the headers
- understand which protocol is being used and display the result
- for wireshark: save all the packets, display them or not according to a display filter

Wireshark configuration

- Edit/Preferences
- Capture/Options
- Capture/Start
- http://www2.hawaii.edu/~esb/2009fall.ics351/wiresharksep01.txt has an example of wireshark output
- http://www2.hawaii.edu/~esb/2009fall.ics351/tcpdumpsep01.txt

  has an example of tcpdump output