Intelligent Network Devices

• Firewall
• Router
• Managed Switch/Bridge
• Wireless Access Point

• Un-intelligent Network devices:
  – Hub
  – Repeater
  – Unmanaged Switch

What info do you need?

What info is relevant to your investigation?

• Firewall logs showing inbound and outbound port and IP connections
• Internal IP address vs. external IP address
• DHCP and/or “attached devices” logs or lease records
• Configuration information for Router, Gateway and/or Wireless Access Point
  – Unsecured WAP?
  – Remote access?

How do I connect to it?

So how do I get information off of it?

• Connect via “console” port (either RJ-45 or DB9)
  – Serial (DB9) connector via straight, rolled or null-modem cable to the serial port on your laptop
  – RJ-45 via same as above to DB9/RJ-45 adapter connected to the serial port on your laptop
• All devices use different combinations or straight vs. null-modem vs. rolled so consult online resources for exact connection.
• Many devices (if configured as such) can be connected to and configured via your web browser by entering the IP address of the device into your address bar.
Cables & Adapters

http://www.bnc.ch/support/techlibrary/serial_cables
1=blue, 2=orange, 3=black, 4=red, 5=green, 6=yellow, 7=brown, 8=gray

Terminal Emulation Program (HyperTerminal)

- Start Hyper-terminal
- Using com port, set to 9600, 8, None, 1 and Flow control usually either Hardware or None.

Capture all activity in a log.

Browser interface?

- Capture your activity and important screen info you wish to document, using screenshots, Camtasia or other similar method.

Questions???

Use the discussion board, as usual…