**Shortest Path First Example**

Example: Received Set of Link State Update Packets
(from Fig. 5-13, Computer Networks)

<table>
<thead>
<tr>
<th>Identity</th>
<th>Sequence #</th>
<th>Age</th>
<th>List of Neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2021</td>
<td>60</td>
<td>B – 4, E – 5</td>
</tr>
<tr>
<td>B</td>
<td>2021</td>
<td>60</td>
<td>A – 4, C – 4, F – 6</td>
</tr>
<tr>
<td>C</td>
<td>2021</td>
<td>59</td>
<td>B – 4, D – 3, E – 1</td>
</tr>
<tr>
<td>D</td>
<td>2020</td>
<td>10</td>
<td>C – 3, F – 7</td>
</tr>
<tr>
<td>E</td>
<td>2020</td>
<td>9</td>
<td>A – 5, C – 1, F – 2</td>
</tr>
<tr>
<td>F</td>
<td>2021</td>
<td>59</td>
<td>B – 6, D – 7, E – 2</td>
</tr>
</tbody>
</table>

Where:
- Sequence number: Only process packets with larger sequence numbers, from any particular node.
- Age: Last packet received is only good for a set duration of time: time is decremented.

Exercise: Construct a Shortest Path First graph from the above information.

![Shortest Path First Graph](image)

**CIDR**

Fill in the blank!

<table>
<thead>
<tr>
<th>Company</th>
<th>First Address</th>
<th>Last Address</th>
<th>Number of Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: 10.6.0.0/22</td>
<td>10.6.0.0</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>B: 10.7.128.0/20</td>
<td>10.7.128.0</td>
<td>10.7.143.255</td>
<td></td>
</tr>
<tr>
<td>C: 10.8.7.0/22</td>
<td></td>
<td>10.8.3.255</td>
<td>1024</td>
</tr>
<tr>
<td>D: 10.9.128.0/21</td>
<td>10.9.128.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**IP Network Addressing**

The configuration, shown below, shows an Autonomous System or network configuration for company AmeridyntechiCorp.

1) Zeus has an IP address of 140.84.2.3: Zeus’s IP address indicates the network is Class_____.

2) Label the nodes as hosts and routers (H or R) inside each box.

3) How large does the Time-To-Live field have to be for a packet to traverse from Ishtar to Apollo?

4) Label all the hosts and routers with appropriate IP addresses. For our class consistency, assume routers get .1 (or lowest) host addresses.

5) An efficient but complete router table for Zeus might show:

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Gen Mask</th>
<th>Next Hop</th>
<th>Flags</th>
</tr>
</thead>
</table>

- **Subnet 1**
  - Apollo

- **Subnet 2**
  - Zeus

- **Subnet 3**
  - Ishtar
**Fragmentation/Reassembly**

An Internet network running IPv4 looks as follows:

![Network Diagram](image)

The two LANs have a maximum layer 2 frame size of 2000 bytes, but the WAN supports a maximum frame payload size of 420 bytes. A datagram of 1000 bytes is to be transmitted from Node A to Node B. Router A detects that the datagram must be fragmented.

The datagram will be reassembled at (circle one:) Router_B or Node_B

Fragmentation of Datagram 45.
The Payload size of 1,000 octets is to be transmitted over the network
The maximum layer 2 frame size is 420 bytes for WAN not including the Layer 2 header.
The IP Header size is 20 bytes.

<table>
<thead>
<tr>
<th>Identification</th>
<th>Fragment 1</th>
<th>Fragment 2</th>
<th>Fragment 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment Length</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fragment Offset</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Fragment Flag</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lab: Using the Wireshark Sniffer

Start up a cmd terminal by selecting the console icon at the top of the screen.

1. Learning Your IP Address

Open a DOS prompt. Then execute the ‘ipconfig’ command to learn your IP address.

Start -> Command Prompt or Start-> Run (with Open: Cmd)

> ipconfig

1a) Your IP Address is:

2. Using a Sniffer

Open the Wireshark sniffer:

Press the Wireshark icon on the desktop or Start->All Programs->Wireshark.
Select Capture-> Options
In the Capture box, select/check Local Area Connection. This should post an IP address.

Configure Wireshark to read only packets destined to your IP address as follows:

Capture Filter: host <your IP address>

We want to capture and display packets in real-time. Optionally you may turn off MAC name translation, because if the processor gets too busy, packets will be lost.

Set all three Display Option check boxes (to select to see packets in real time).

Press Start (and if necessary, Continue without Saving)

The sniffer is now started and we need to generate data to observe. At the DOS command prompt enter:

> ping ginger.cs.uwp.edu

Observe a series of Ping requests and replies. To observe the contents of the Ping packets:

Click on a Echo (Ping) Request packet.

In the second box you will see details of different layers of the protocol.
Expand [+ ] Internet Protocol
Expand [+ ] Flags (within the IP header)

You can scroll up and down using the arrow keys on any line of the Wireshark display.

2a) What is the Windows default Time-to-Live for a Ping message?

2b) What is the More Fragment flag set to?

3. Observing Fragments

Linux is required to do this exercise. Open a terminal using the screen icon. Send ping messages to the Windows XP terminal with a length of 5000 bytes:

$ ping <Your IP address> -s 5000

Now observe what Wireshark has caught. You should see a number of ICMP Echo (ping) Requests followed by 3 IP fragments. The ICMP packet contains the ICMP header. The following three packets include the fragmented data. (You can ctl-C out of the ping on the Linux system so that the Ping transmissions stop.) In Wireshark, click on the ICMP packet and the following IP packets to observe packet contents. Answer the following questions:

3a) What is the standard Linux Ping Time-to-Live?

3b) What is the More Fragment flag in the last packet?
3c) What is the Fragment Offset in the second packet?

4. **Observing DNS packets and Traceroute**

At windows prompt enter:  
> tracert ginger.cs.uwp.edu

4a) What are the Time-To-Live fields set to in the Ping requests?

Look at the ICMP Time-to-Live Exceeded packets which lists the routers on the path to ginger.cs.uwp.edu. The IP protocol Source Address lists the router which encountered the failed Time-To-Live.  
4b) What is the IP address of the routers on the path to ginger?

4c) What is the Type of ICMP message for Time-To-Live Exceeded?

Scroll up (using arrow keys) to a DNS Standard Query for ginger.cs.uwp.edu. This message is requesting a translation of ginger.cs.uwp.edu to an IP address (number).  
Expand (+) the Domain Name System (query)  
Expand (+) the Query part

4d) What is included in the Query part?

Look at the Query Response message, and expand (+) its Answer section.  
4e) What is the IP address?

5. **DNS and ICMP Errors**

Now attempt to ping the following machines:  
> ping robot.cs.uwp.edu (does not exist)  
> ping eaglet.cs.uwp.edu (powered off)

5a) What happened in each case?  
   Robot  
   Eaglet