Fundamentals of Internetworking
We define "Internetworking" as the science/black art of connecting different networks together.
Fundamentals of Internetworking

- **Target Audience:**
  - Networking professionals with a basic understanding of local area networking.

- **Objectives:**
  - The purpose of this class is to provide a basic understanding of internetworking and the basis for further training to help you sell and support internetworking equipment.
  - At the end of this class, you should understand how routers work in an internetwork.
Course Outline

- Layer 2 Ethernet Basics
- Layer 2 (Ethernet) Interconnection Devices
- Layer 3 - The Network Layer
- Wide Area Networking
- Bridges vs. Switches vs. Routers
- IPX Addressing and Forwarding
- IP Addressing and Forwarding
- Router Configuration
Layer 2 Ethernet Basics
 OSI Seven Layer Model

- Each layer has specific purposes (navigation, error recovery, etc.) and has a virtual conversation with its partner defined by the layer protocol.

- Layer 2 or the Data Link Layer defines how we navigate on a specific network. Layer protocol: Ethernet, Token Ring, FDDI, etc.

- Layer 3 or the Network Layer defines how we navigate between networks. Layer protocol: IP, IPX, etc.
The transmitting node has data to send to the receiving node. Each layer adds its own header or header/trailer to the data and passes it to the next layer.

The header/trailer for each layer is defined in the layer protocol and is the virtual conversation between partners.

Both layer 2 and layer 3 have source and destination addresses in their headers because both layers are responsible for navigation.
Ethernet LANs

- Ethernet is a multi-access broadcast type network.
- Each node or host has an address called the Ethernet, station, hardware, or MAC (Media Access Control) address.
- Addresses are flat (not hierarchical); that is, carry no information about location. Analogy: phone numbers within an area code and prefix. Example: (916) 787-XXXX
10Base5 and 10Base2
- uses coaxial cable
- physical bus topology

10BaseT and 100BaseVG
- uses twisted pair wiring and hubs or concentrators
- physical star topology
- logical bus topology

Fiber Optic InterRepeater Link (FOIRL)
- uses fiber optic cable
- distances up to 2 km
- physical star topology
- logical bus topology
Ethernet Addressing

- Each frame is addressed with the source and destination addresses.
- Frames with a specific destination address are called unicast frames.
- Special addresses: Broadcast Multicast
Media Access and Collisions

- Media access control for 10Base5, 10Base2, and 10BaseT is Carrier Sense Multiple Access / Collision Detect (CSMA/CD).
  - Access is statistical and collisions occur when two devices transmit at the same time.

- Access for 100BaseVG is Demand Priority Protocol (DPP).
  - Access is deterministic and no collisions can occur.
Layer 2 (Ethernet)
Interconnection Devices
Interconnecting LAN Segments: Repeaters

- Plug-and-play
- Transparent
- Forwards all traffic with no error checking.
- 10BaseT hubs act as multi-port repeaters
Interconnecting LAN Segments: Learning Bridges

- Plug-and-play
- Transparent
- Store-and-forward device
- Does not forward errored packets
- Segments collision domains

✓ Transparent
✓ Store-and-forward
Interconnecting LAN Segments: Bridges: Traffic Segmentation

- Builds forwarding table by looking at source address.
- Forwards or filters packet based on forwarding table.
- Treats each node as an individual.
- Bridge Philosophy: "If in doubt, flood it."
- Multiport bridges
Interconnecting LAN Segments: Switches

- Similar to multiport bridge
  - Plug-and-play
  - Forwarding based on Ethernet address
- Simultaneous connections
- Cut-through or store and forward
  Multiplies bandwidth

✓ Cut-through
Layer 3 - The Network Layer
Layer 3 Addressing

- Layer 3 addressing is hierarchical. This means that the address carries some information about how things are grouped. Analogy is a phone number: area code and number.

- A complete layer 3 address is made up of two parts: the network address and the host or node address.

- Layer 3 addressing is independent of layer 2 media type.
Layer 3 Addressing: Fictional Layer Three Protocol

- Fictional Layer Three Protocol (FLTP) addressing (like all layer 3 protocols) has two parts: the network part and the node part.

- Addresses are written as **XXX.Y**, where XXX is the network part of the address and Y is the node part of the address.
Routers and Layer Three Addressing

- Networks are separated by routers.
- Each interface of a router has its own layer 3 address on the network.
- Control and security can be easily handled as a group instead of individually like layer 2 devices.
Routers build routing tables based on their own configuration and information from other routers.

Routers forward packets by looking at the layer 3 destination address, finding that address in the routing table, and forwarding the packet to the next hop or node.

Router Philosophy: "If in doubt, drop it."
Wide Area Networking
Wide Area Networks

- In our context, wide area networking is using wide area links to interconnect LANs.
- Routers support virtually all WAN link types and WANs are one of the main uses of routers.
Point-to-Point Links

- Synchronous digital or analog circuit (RS-232, RS-442, or V.35).
- Analog speed: up to 115 Kbps
- DDS (Digital Data Service): up to 56 Kbps
- Fractional and T1: up to 1.544 Mbps
- Cost is typically fixed rate.
Circuit Switched Links (PSTN, ISDN, Switched 56)

- Connection is established only when needed.
- Demand Circuits
  - Dial-Backup
  - Dial-on-Demand
  - Bandwidth-on-Demand
- Typically requires special configuration.
- Cost is usually a subscription fee and usage fee.
Packet Switched Networks (X.25 and Frame Relay)

- Each packet is addressed and sent through the cloud via a "virtual circuit".
- A permanent virtual circuit (PVC) emulates a point-to-point link. A switched virtual circuit (SVC) emulates a switched link.
- Frame Relay is the fastest growing link type in US.
- X.25 is still in wide-spread use in Europe.
- Cost can be usage-based or fixed.
Bridges vs. Switches vs. Routers
Bridges

- **Best for:**
  - Local traffic segmentation

- **Advantages:**
  - Plug-and-play operation
  - Resets the repeater count
  - Simple Filtering

- **Limitations:**
  - WAN capability
  - Broadcast control
  - Traffic filtering
  - Security
Switches

- Best for:
  - Dedicating/multiplying bandwidth to servers

- Advantages:
  - Plug-and-play operation
  - Low latency

- Limitations:
  - No WAN capabilities
  - Broadcast control
  - Traffic filtering
  - Security
Routers

- Best for:
  - Wide Area Networking
  - Traffic filtering
    - Security/firewalls
    - Limiting the amount of unnecessary WAN traffic
  - Connecting dissimilar media types

- Advantages:
  - Redundant, load sharing links
  - Can also function as a bridge

- Limitations:
  - Complexity
  - Latency (dependent on speed of the router)
IPX Addressing and Forwarding
IPX Addressing

- An IPX address is 10 octets in length.
- The network address is fixed at 4 octets. This gives 4.29 billion networks.
- The node address is fixed at 6 octets and uses the MAC address. This gives 281 trillion nodes.
- IPX addresses are written in hexadecimal, usually with a colon between the parts.
  - Example: BAABAA01:0800091FC2AB
Forwarding IPX packets

Example Configuration

Client: Dilbert
Client Network: BADCAFE1

Server: Dogbert
Server Network: FACE0FF6
Forwarding IPX packets

Example Configuration:
Internal Network Number

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>BADCAFE1</td>
<td>1</td>
<td>Own MAC</td>
</tr>
<tr>
<td>FACE0FF6</td>
<td>2</td>
<td>Own MAC</td>
</tr>
<tr>
<td>BAABAA01</td>
<td>2</td>
<td>Dogbert Mac</td>
</tr>
</tbody>
</table>
Forwarding IPX packets

- Dilbert needs to send some data to Dogbert.
- Dilbert knows Dogbert’s IPX network address and the router’s MAC address. How Dilbert knows that is beyond the scope of this class.
- Dilbert builds the layer 2 and layer 3 headers and sends it to the router.
- The router receives the packet and finds the destination address in its route table.

Routing Table

<table>
<thead>
<tr>
<th>Network</th>
<th>Interface</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>BADCAFE1</td>
<td>1</td>
<td>Own MAC</td>
</tr>
<tr>
<td>FACE0FF6</td>
<td>2</td>
<td>Own MAC</td>
</tr>
<tr>
<td>BAABAA01</td>
<td>2</td>
<td>Dogbert Mac</td>
</tr>
</tbody>
</table>

```
<table>
<thead>
<tr>
<th>Router MAC</th>
<th>Dilbert MAC</th>
<th>BAABAA01: 00000000000001</th>
<th>BADCAFE1: Dilbert MAC</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Forwarding IPX packets

- Based on the destination address, the next hop is the internal router on the server.
- The router changes the layer 2 addresses and forwards the packet to Dogbert.
- Layer 3 addresses do not change.
IP Addressing and Forwarding
IP Addressing

- An IP Address is 4 octets (bytes) or 32 bits in length.
- It is written in "dotted decimal" format.
  - Example: 192.130.10.121
  - Value of each octet is converted to decimal and separated by dots or periods.
    - First octet is 192 or 11000000
    - Second octet is 130 or 100000010
    - Third octet is 10 or 00001010
    - Fourth octet is 121 or 01111001
    - Binary address is: 11000000.100000010.00001010.01111001
IP Addressing: Address Classes

- The total IP address space is split into classes.

- The class of an address is determined by looking at the first bits of the first octet.

<table>
<thead>
<tr>
<th>Class</th>
<th>First Octet</th>
<th>Decimal Range of First Octet</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>0</td>
<td>1-127</td>
<td>10.24.224.191</td>
</tr>
<tr>
<td>Class B</td>
<td>1 0</td>
<td>128-191</td>
<td>134.251.77.108</td>
</tr>
<tr>
<td>Class C</td>
<td>1 1 0</td>
<td>192-223</td>
<td>212.145.37.201</td>
</tr>
</tbody>
</table>
IP Addressing: Address Classes

- An IP address has two parts: the network part and the host part.
- The different classes have different lengths for the network part (and therefore the host part) of the address.
- The network part of IP addresses is registered with the Internet Network Information Center or InterNIC to ensure they are unique.

<table>
<thead>
<tr>
<th>Class</th>
<th>Number of Networks</th>
<th>Number of Hosts per Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>127</td>
<td>16,777,214</td>
</tr>
<tr>
<td>Class B</td>
<td>16,383</td>
<td>65,534</td>
</tr>
<tr>
<td>Class C</td>
<td>2,097,151</td>
<td>254</td>
</tr>
</tbody>
</table>
### IP Addressing

#### Example IP Addresses:

<table>
<thead>
<tr>
<th>Address</th>
<th>Class</th>
<th>Network</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>191.254.1.111</td>
<td>_____</td>
<td>___________</td>
<td>_____</td>
</tr>
<tr>
<td>132.253.125.201</td>
<td>_____</td>
<td>___________</td>
<td>_____</td>
</tr>
<tr>
<td>15.24.225.61</td>
<td>_____</td>
<td>___________</td>
<td>_____</td>
</tr>
<tr>
<td>195.67.158.1</td>
<td>_____</td>
<td>___________</td>
<td>_____</td>
</tr>
<tr>
<td>129.192.192.10</td>
<td>_____</td>
<td>___________</td>
<td>_____</td>
</tr>
</tbody>
</table>
Subnet Addressing

- Let’s say you are designing a network for a company that has 120 different sites each with between 150 and 250 nodes (total of about 24,000 nodes).

- How many class A addresses would you need?
  - class B?
  - class C?

- Which would you ask for?

- Subnetting provides a method for breaking large networks into smaller ones.
Subnet Addressing

- The Subnet Mask allows the network designer to redefine what part of the address is the network and what part is the host.

- The subnet mask is written in dotted decimal like the IP address. The "ones" part represents the network part of the address and the "zeros" part represents the host part of the address.

- Consider addresses:
  - 134.215.145.10
  - 134.215.210.1
The subnet mask can split the address at any bit.

To calculate the number of networks or hosts: 
\((2^{\# \text{ of bits}}) - 2\)

### Class B and Subnet Mask

<table>
<thead>
<tr>
<th>Subnet Mask</th>
<th>Networks</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>134 251</td>
<td>2046</td>
<td>30</td>
</tr>
<tr>
<td>255 255 255 224</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Class C and Subnet Mask

<table>
<thead>
<tr>
<th>Subnet Mask</th>
<th>Networks</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>212 145 37</td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td>255 255 255 224</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forwarding IP packets

Example Configuration

Host: Dilbert
IP Address: 134.215.11.27
Default Gateway: 134.215.11.1

Host: Dogbert
IP Address: 134.215.35.99
Default Gateway: 134.215.35.1

Network: 134.215.11
Subnet Mask: 255.255.255.0
IP Address: 134.215.11.1

Network: 134.215.35
Subnet Mask: 255.255.255.0
IP Address: 134.215.35.1

Routing Table

Network  Next Hop
134.215.11  134.215.11.1
134.215.35  134.215.35.1
Forwarding IP packets

- Dilbert ARPs for the MAC address of the default gateway
- Dilbert sends the packet to the router (via layer 2).
- The router receives the packet and looks in its routing table for a route to the IP destination network.
Forwarding IP packets

- The route table tells the router what the next hop is.
- The next hop is the router’s own interface on the destination network. The router ARPs for the Dogbert’s MAC address.
- The router changes the layer 2 addresses and forwards the packet to Dogbert.
Forwarding IP packets

- This is the two hop case and is more general.
- Router 1 receives the packet from Dilbert.
- The next hop to the destination network is Router 2. Router 1 sends the packet to Router 2.
- Router 2 receives the packet from Router 1 and forwards the packet to Dogbert.
Routing Protocols

- Each router knows what networks it is connected to through its configuration.
- In order to build their routing table, routers use a "routing protocol" to exchange information with each other about what networks each router can reach.
- This information is used to build the routing table.
- RIP
- OSPF
RIP: Routing Information Protocol

- RIP is a distance metric protocol.
- Each router broadcasts at regular intervals (typically 1 minute) what networks it can reach and how many hops away the network is for that router.
- This broadcast frequency was used to provide fast "convergence" in a LAN environment where the traffic volume didn’t matter much, but can generate a significant amount of traffic across slow WAN links.
OSPF: Open Shortest Path First

- OSPF is a link state protocol.
- Initially, each router broadcasts all routes it knows about.
- After reaching convergence, each router broadcasts only the changes it detects in the network.
Router Configuration
Router Configuration: Console Port

- To configure a router (all but the 210), connect a "null-modem" cable from the router console port to a VT-100 terminal or PC (using Windows terminal).

- The Router 210 uses Stack Manager.
Console Port:
Windows Menu

PRESS: ? for help, Down, Up, <- to exit, <RETURN> to select
Console Port: Terminal Parameters

**Terminal Emulation**
- ITY (Generic)
- DEC VT-100 (ANSI)
- DEC VT-52

**Terminal Preferences**
- Terminal Modes
  - Line Wrap
  - Local Echo
  - Sound
- CR → CR/LF
- Inbound
- Outbound
- Cursor
  - Block
  - Underline
  - Blink

**Communications**
- Baud Rate
  - 110
  - 300
  - 600
  - 1200
  - 2400
  - 4800
  - 9600
  - 19200
- Data Bits
  - 5
  - 6
  - 7
  - 8
- Stop Bits
  - 1
  - 1.5
  - 2
- Parity
  - None
  - Odd
  - Even
  - Mark
  - Space
- Flow Control
  - Xon/Xoff
  - Hardware
  - None
- Connector
  - None
  - COM1:
  - COM2:
  - Parity Check
  - Carrier Detect

**Translations**
- Courier
- Courier Net
- Fixedsys
- United Kingdom
- Denmark/Norway
- IBM to ANSI
- Show Scroll Bars
- Buffer Lines: 100
- Use Function, Arrow, and Ctrl Keys for Windows
Router 210 Configuration

From within Stack Manager, click on the Router Icon.
Router Configuration: Main Menu

---

SESSION 2 - MGR MODE

Main Menu

--> 1. Statistics Screen Menu
2. Network Control Language Interpreter
3. Configuration Editor
4. Event Log
5. LOGOUT
6. Quick Configuration
7. Quick Remote
8. SmartBoot Helper

PRESS: ? for help, Down, Up, <- to exit, <RETURN> to select
Router Configuration:
Quick Config

Choose a system name for your router. The name should be less than 16 characters long and should not contain any spaces.
Ethernet Interface:
IP Address

Enter an IP address if you wish to route DoD IP traffic through this port. Use 'dotted decimal' notation X.X.X.X where each X is a decimal number between 0 and 255. Even if you are not routing IP traffic, you need to configure IP if you have SNMP or inbound Telnet enabled, or you wish to use outbound Telnet.
Ethernet Interface: Subnet Mask

Enter the subnet mask for this port in `dotted decimal' notation. The subnet mask determines what portion of the above IP address is the subnetwork number and what portion is the host number.
Ethernet Interface:
IPX Address

<table>
<thead>
<tr>
<th>Ethernet 1</th>
<th>134.215.11.1</th>
<th>255.255.255.0</th>
</tr>
</thead>
</table>

Enter an IPX network number to enable Novell IPX routing through this port. It should be a hexadecimal number from 1 to FFFFFFFFE that is unique throughout your entire Novell internet.
WAN Interface:
IP Address

<table>
<thead>
<tr>
<th>Ethernet 1</th>
<th>134.215.11.1</th>
<th>255.255.255.0</th>
<th>BADCAFE1</th>
</tr>
</thead>
</table>

Enter an IP address if you wish to route DoD IP traffic through this port. Use "dotted decimal" notation X.X.X.X where each X is a decimal number between 0 and 255. Even if you are not routing IP traffic, you need to configure IP if you have SNMP or inbound Telnet enabled, or you wish to use outbound Telnet.
**WAN Interface:**

**Subnet Mask**

---

<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>Settings</th>
<th>Phone</th>
<th>Transfers</th>
<th>Help</th>
</tr>
</thead>
</table>

**HP 27285A Router ER**  
**ROUTER_1**  
**6-Jul-1993**  
**4:52:31**

---

**SESSION 2 - MGR MODE**

Subnet mask: 255.255.255.0

---

Use arrow keys to move, / for hot keys -

**System name:** ROUTER_1  
**IP host-only:** NO  
**SNMP enabled:** YES  
**Inbound Telnet enabled:** YES

<table>
<thead>
<tr>
<th>Ethernet 1</th>
<th>Ethernet 2</th>
<th>WAN 1</th>
<th>WAN 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Brig</strong></td>
<td><strong>Enab</strong></td>
<td><strong>IP</strong></td>
<td><strong>IP</strong></td>
</tr>
<tr>
<td><strong>DoD IP</strong></td>
<td><strong>Address</strong></td>
<td><strong>Subnet Mask</strong></td>
<td><strong>Network</strong></td>
</tr>
<tr>
<td>134.215.11.1</td>
<td>255.255.255.0</td>
<td>BADCAFE1</td>
<td></td>
</tr>
</tbody>
</table>

---

Enter the subnet mask for this port in `dotted decimal` notation. The subnet mask determines what portion of the above IP address is the subnetwork number and what portion is the host number.
### WAN Interface:

**IPX Address**

![Network Configuration Interface](image)

<table>
<thead>
<tr>
<th>System name:</th>
<th>ROUTER_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP host-only:</td>
<td>No</td>
</tr>
<tr>
<td>SNMP enabled:</td>
<td>Yes</td>
</tr>
<tr>
<td>Inbound Telnet enabled:</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet 1</th>
<th>134.215.11.1</th>
<th>255.255.255.0</th>
<th>BADCafe1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAN 1</td>
<td>134.215.77.1</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>WAN 2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter an IPX network number to enable Novell IPX routing through this port. It should be a hexadecimal number from 1 to FFFFFFFE that is unique throughout your entire Novell internet.
Quick Config:
Save Config

<table>
<thead>
<tr>
<th>Ethernet 1</th>
<th>Ethernet 2</th>
<th>WAN 1</th>
<th>WAN 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brg</td>
<td>Enab</td>
<td>134.215.11.1</td>
<td>134.215.77.1</td>
</tr>
<tr>
<td>DoD IP</td>
<td>Address</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>SNMP enabled</td>
<td>YES</td>
<td>IPX Port</td>
<td>Network Parameters</td>
</tr>
<tr>
<td>Inbound Telnet enabled</td>
<td>YES</td>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>IP host-only</td>
<td>NO</td>
<td>WAN Port</td>
<td></td>
</tr>
</tbody>
</table>

Answer yes to save this configuration and exit. Answer no to make more changes to the configuration you have built so far, or to exit without keeping these changes.
Quick Config:
Reboot

<table>
<thead>
<tr>
<th>System name:</th>
<th>ROUTER_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP host-only:</td>
<td>NO</td>
</tr>
<tr>
<td>Brg</td>
<td>DoD IP</td>
</tr>
<tr>
<td>Enab</td>
<td>Address</td>
</tr>
<tr>
<td>Ethernet 1</td>
<td></td>
</tr>
<tr>
<td>Ethernet 2</td>
<td></td>
</tr>
<tr>
<td>WAN 1</td>
<td></td>
</tr>
<tr>
<td>WAN 2</td>
<td></td>
</tr>
</tbody>
</table>

After saving the configuration changes, you must restart the router (reboot) to make them take effect.
Answer yes to reboot immediately.