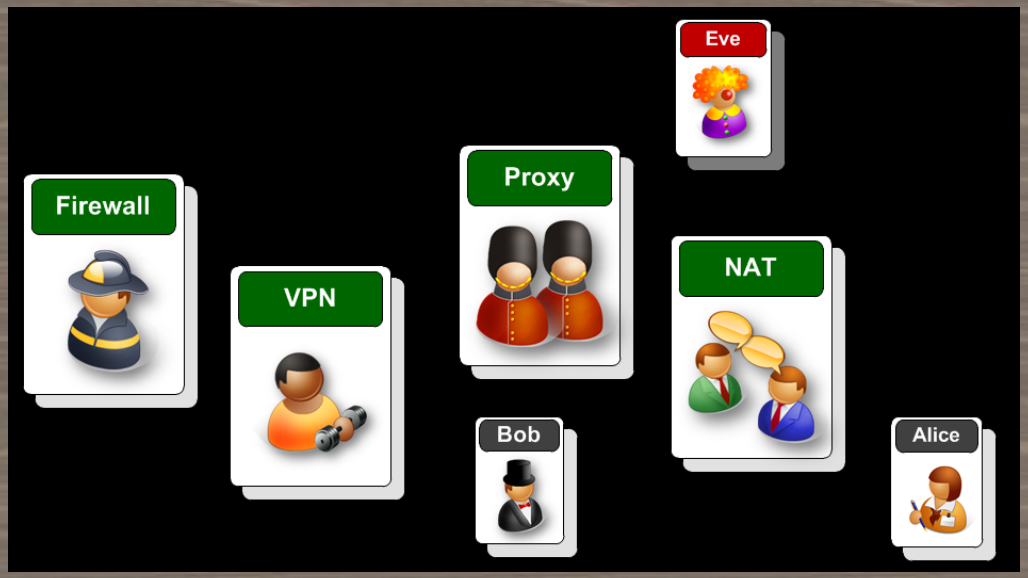
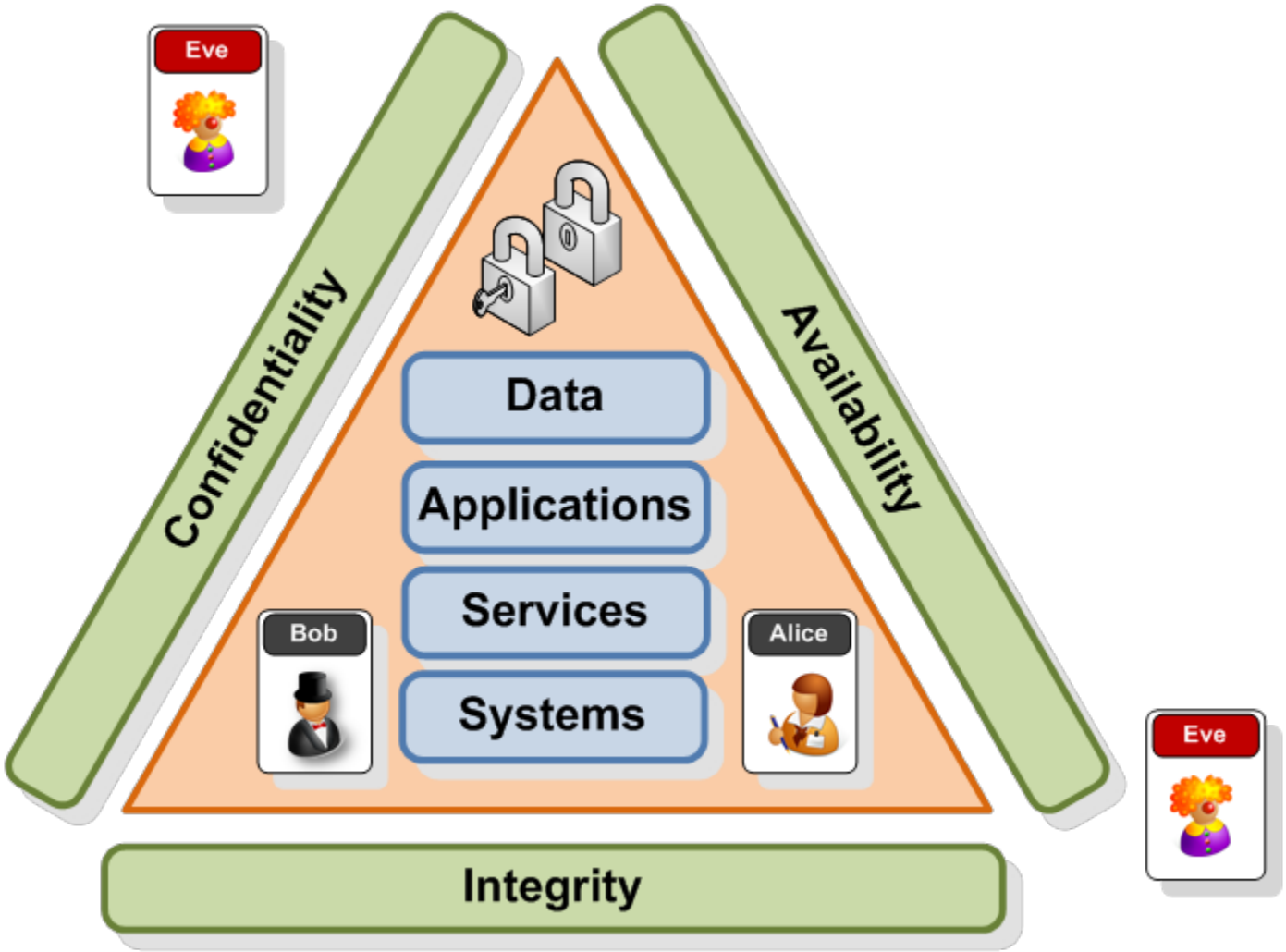
Cyber Workshop

Introduction to Network Security

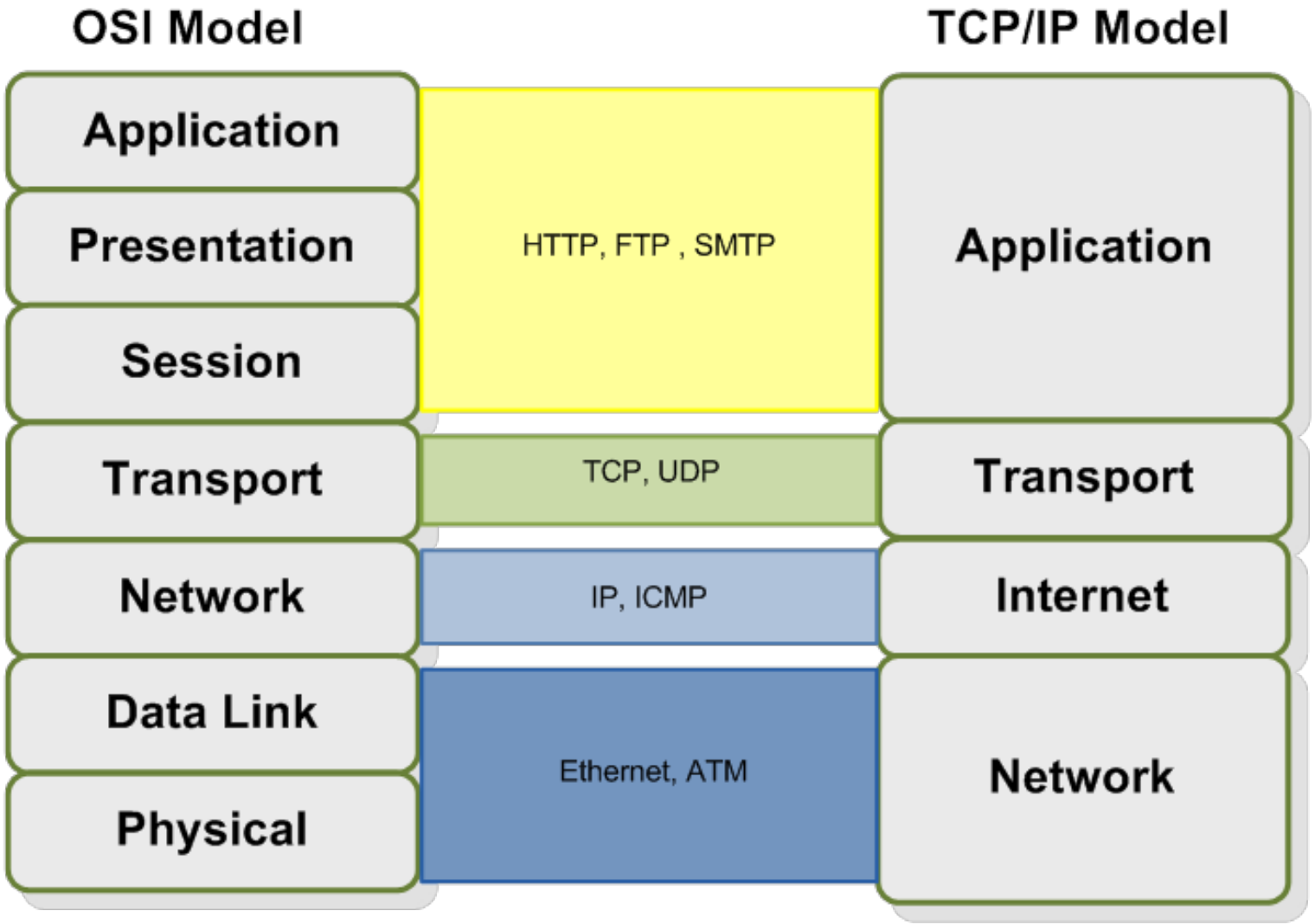
Robert Ludwiniak



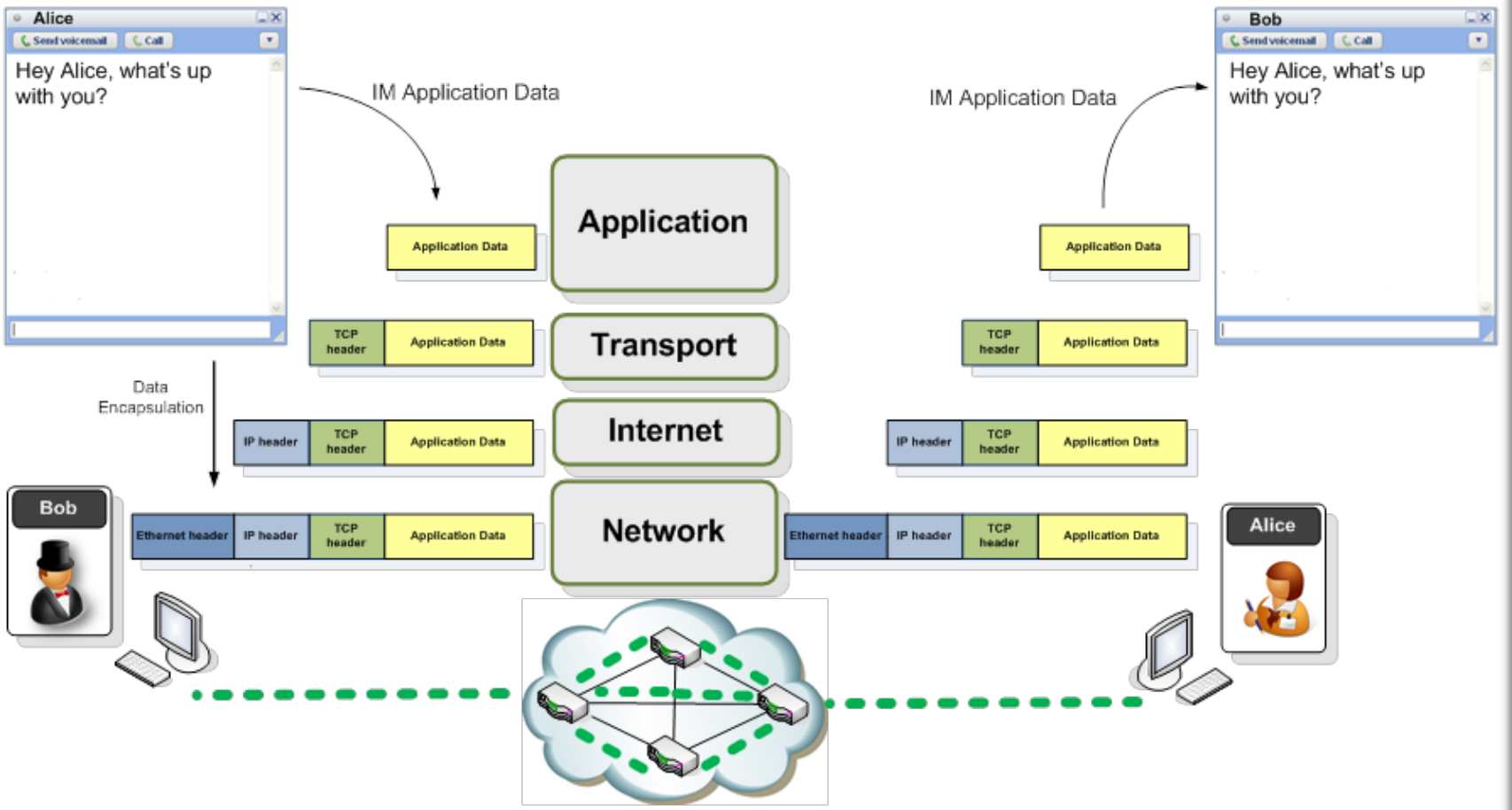
Key Principle Behind Security



Networking – Layer Approach



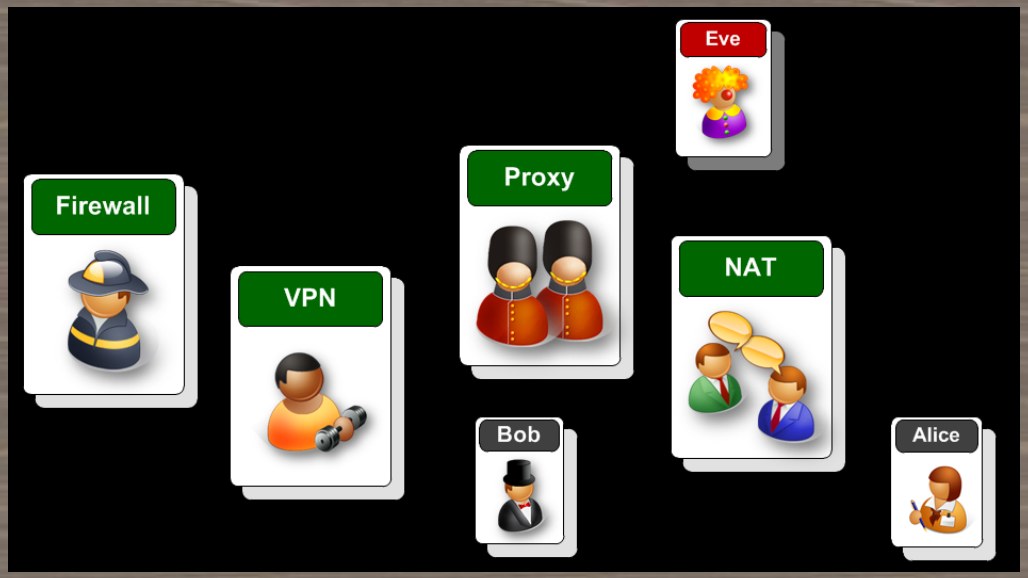
Data Exchange (Encapsulation)



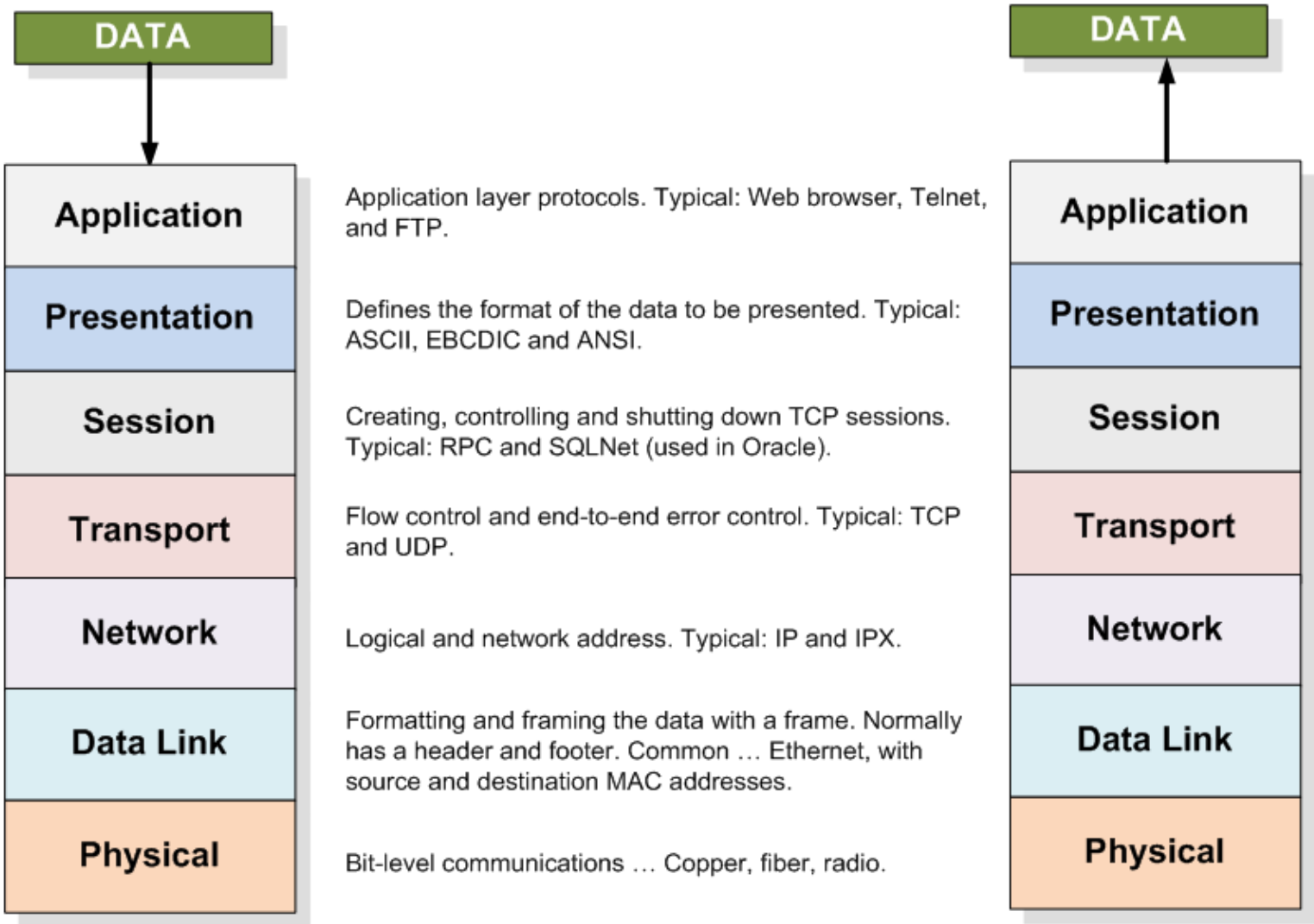
CSN11111 – Network Security

Basic Networking Concepts

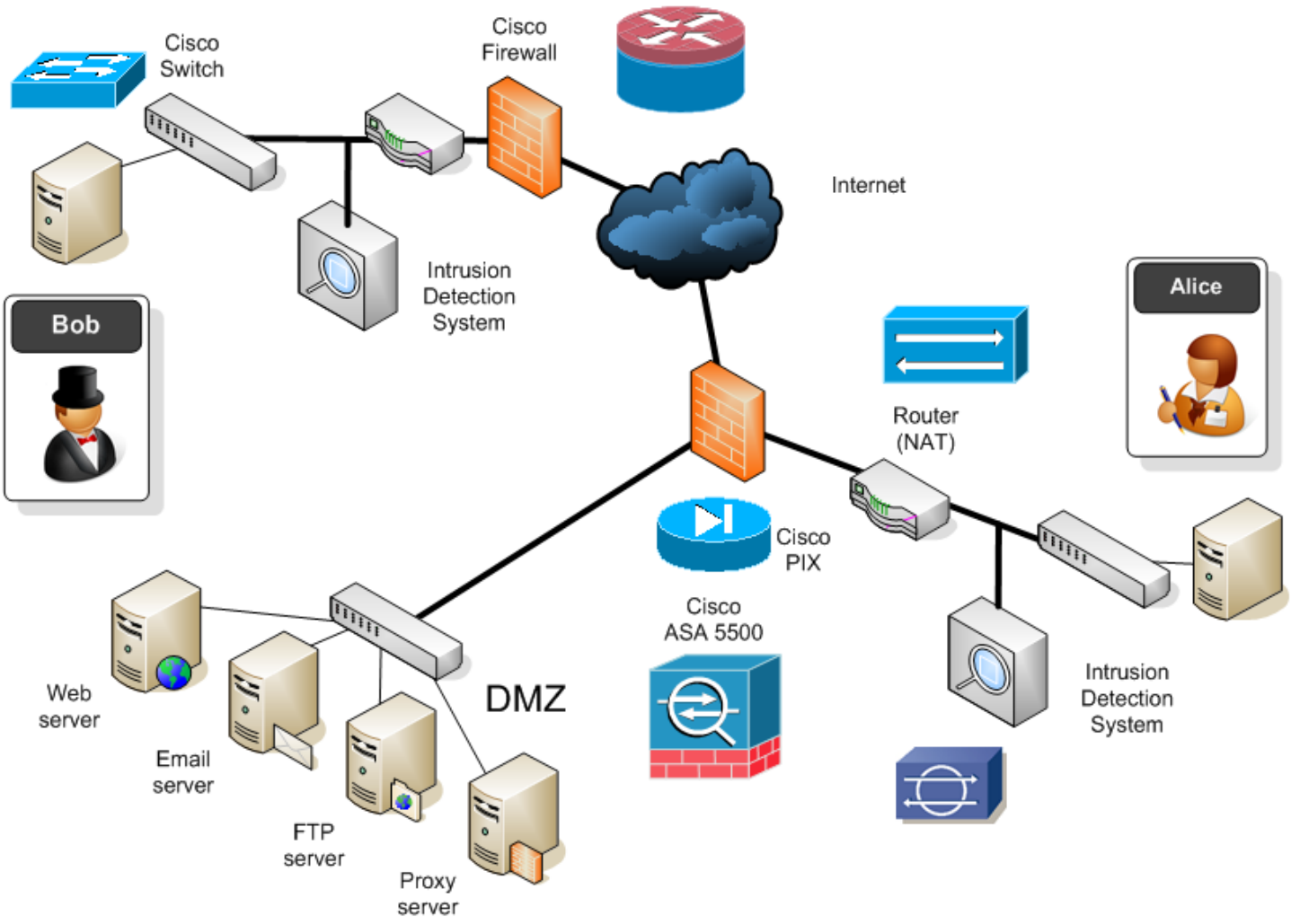
Robert Ludwiniak



Networking Protocols



Example Infrastructure



Ethernet, IP and TCP

Protocol:
1 – ICMP
6 – TCP
8 – EGP
17 - UDP

IP header

Version	Header len.	Type of service
Total length		
Identification		
0	D	M	Fragment Offset
Time-to-live (TTL)		Protocol
Header Checksum		
Source IP Address		
Destination IP Address		

TCP header

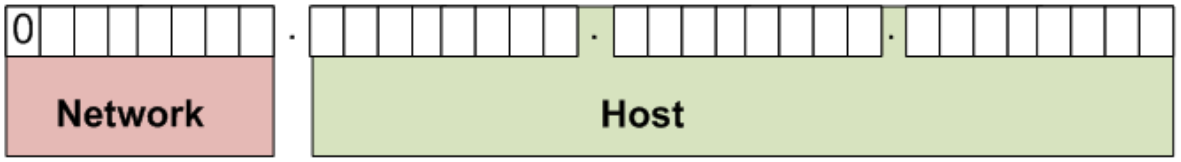
TCP Source Port	
TCP Destination Port	
Sequence Number	
Acknowledgement Number	
Data Offset	Flags/Reserved
Window	
Checksum	
Urgent Pointer	

Preamble (7 bytes)	Start (1 B)	Dest. MAC (6 bytes)	Src. MAC (6 bytes)	Type (2 bytes)	data...	Checksum (4 bytes)

Type:
0x800 – IP
0x806 – ARP

Ethernet frame

Network IP Address

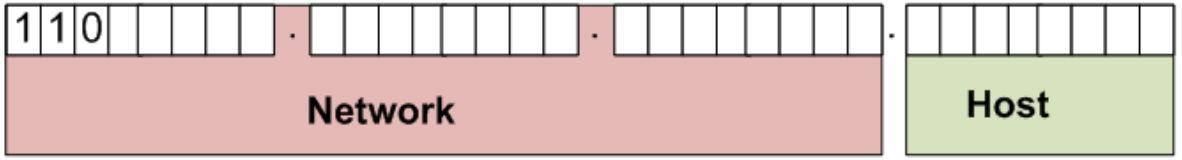


Class A

0.0.0.0 to 127.0.0.0 Networks: 126, Host: 16,277,214
Subnet: 255.0.0.0

Class B

128.0.0.0 to 191.255.255.255 Networks: 16,384, Hosts: 65,534
Subnet mask: 255.255.0.0

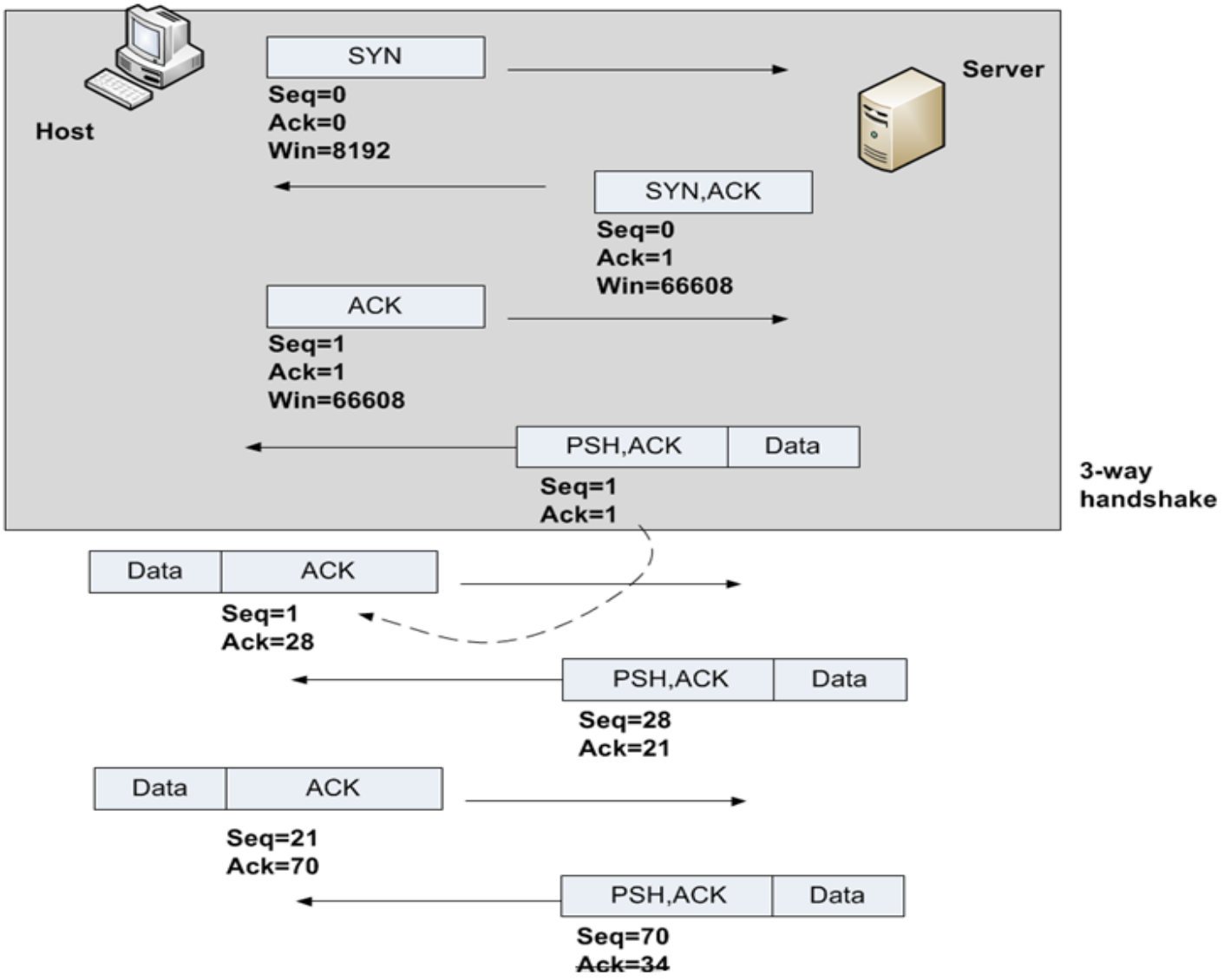


Class C

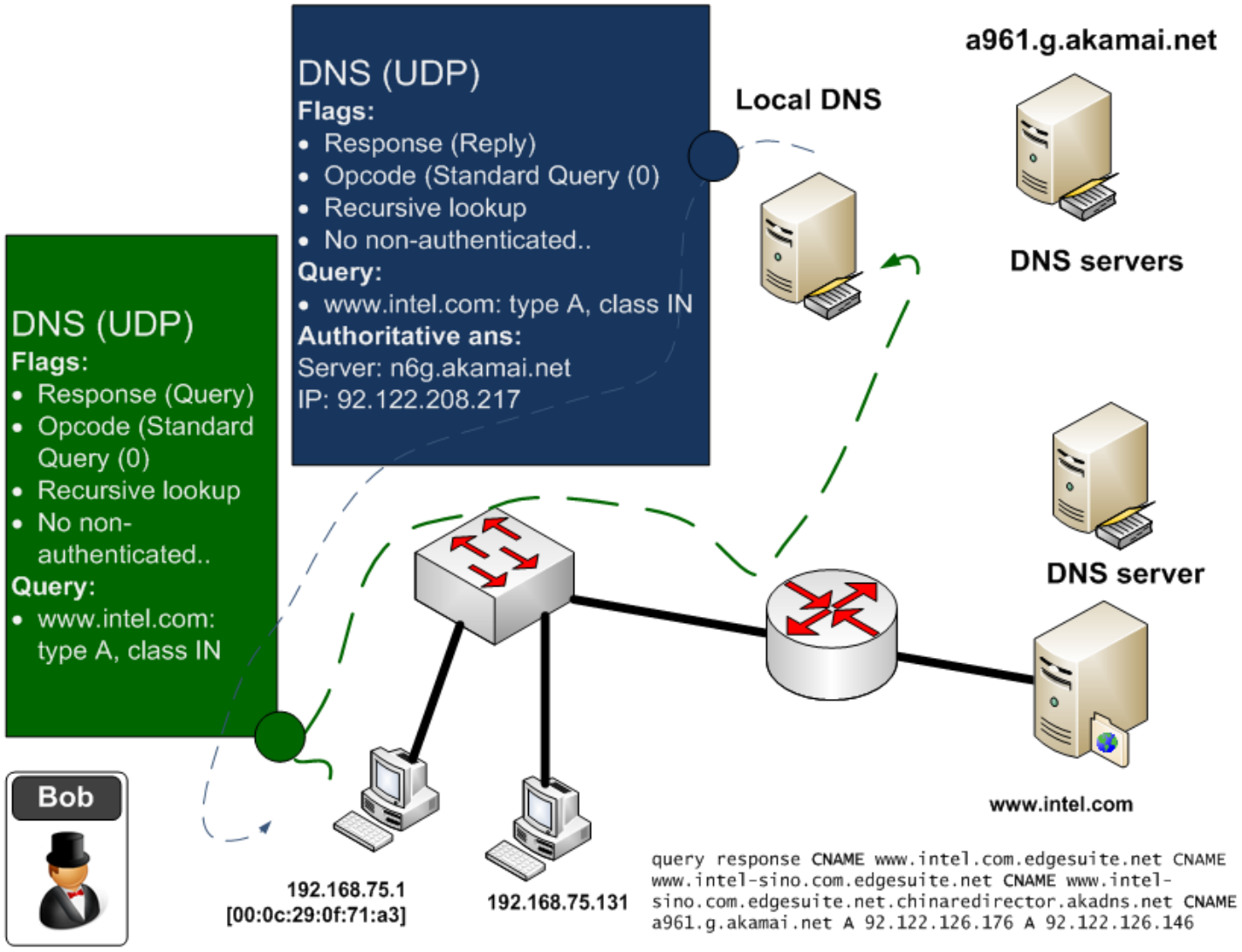
192.0.0.0 to 223.255.255.255, Networks: 2,097,152, Hosts: 254
Subnet mask: 255.255.255.0

Class D: 224.0.0.0- 239.255.255.255
Class E: 240.0.0.0- 255.255.255.255

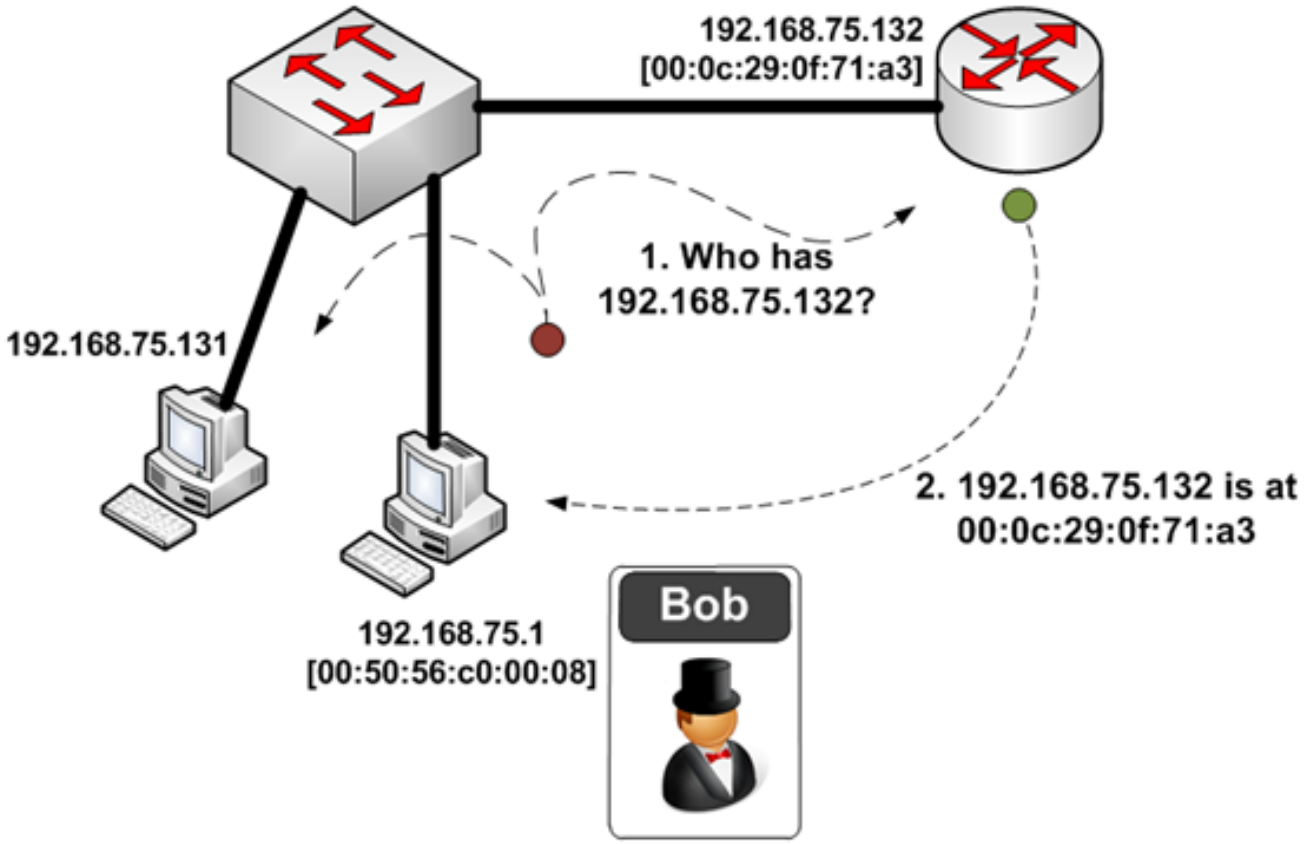
TCP – Client/Server



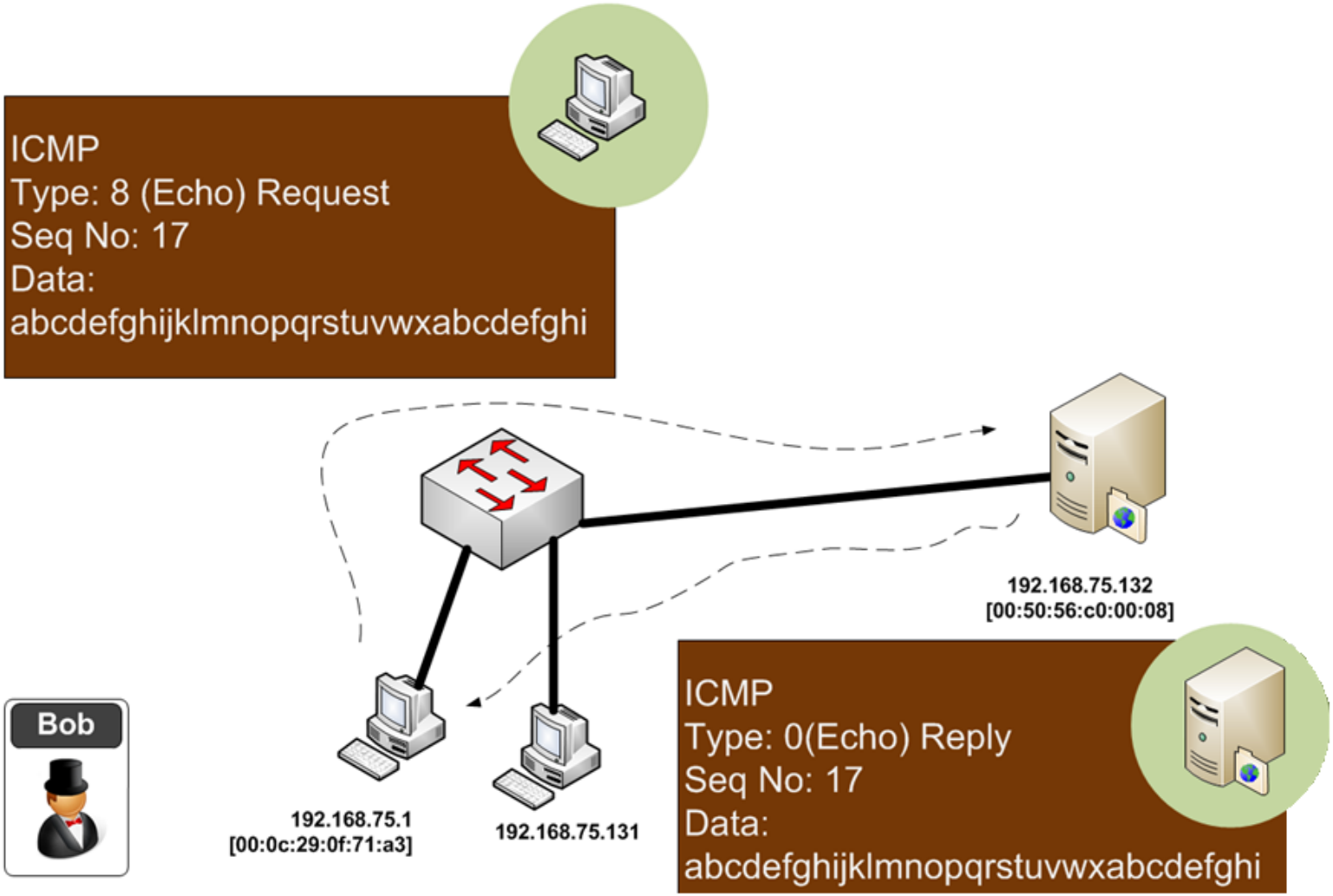
DNS Operation



ARP Operation



ICMP Operation



HTTP Operation

```
HTTP/1.1 200 OK
Content-Length: 2606
Content-Type: text/html
Content-Location: http://192.168.75.132/
<HTML>TEST</HTML>
```

```
GET /info/page.html
```
Retrieve a URL

```
HEAD /info/page.html
```
Just get the header info

```
POST /info/page.html
```
Accept the entity

```
PUT /info/page.html
```
Store entity in an exist resource

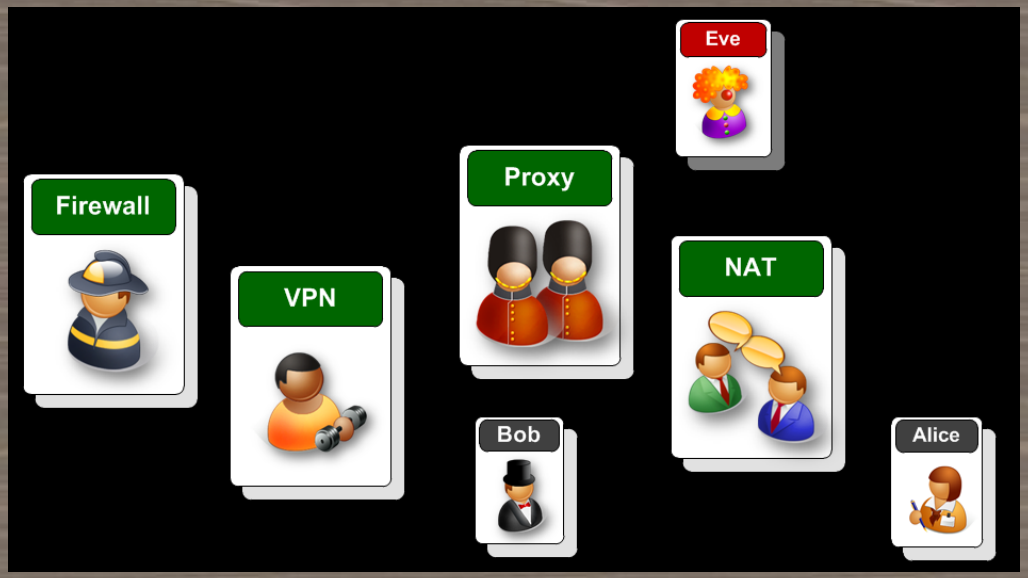
```
Content-type: Image/jpg, image/gif
If-Modified-since: 06 Mat 2013 12:00:00
Host: localhost
Connection: Keep-alive
Accept-language: en-gb
Accept-encoding: gzip, deflate
```


```
RESPONSE:

2xx Successful
200 OK
202 Accepted

3xx Redirection
301 Moved Permanently

4xx Client Error
400 Bad Request
401 Unauthorized
403 Forbidden
404 Not found

5xx Server Error
501 Bad Gateway
```

Cyber Workshop

Networking Devices

Robert Ludwiniak



Networking Devices - Cisco

2811 Router

7206 Router

PIX 515E Firewall

ASA 5510 Firewall

Networking Device Interfaces

- Devices configurable Interfaces
- Interfaces grouped onto cards or ‘slots’

Networking Device Interfaces

Ethernet Interface

Module 1

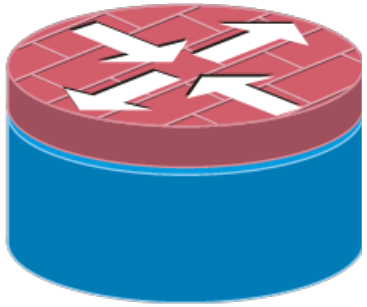
Module 0

Serial Interface (slot 0, 1, 2, 3)

```
Router(config)#interface name module/slot/port
Router(config)#interface serial 0/0/0
```

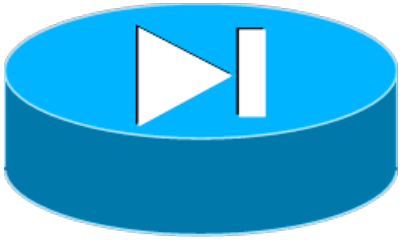
Network Devices - Switches

Cisco Devices - Symbols



Router with Firewall

Router



PIX/ASA Firewall

Switch

Configuration

- A basic router configuration should contain the following:
  - Router name - Host name should be unique
  - Banner - At a minimum, banner should warn against unauthorized use
  - Passwords - Use strong passwords
  - Interface configurations - Specify interface type, IP address and subnet mask. Describe purpose of interface. Issue no shutdown command. If DCE serial interface issue clock rate command.
- After entering in the basic configuration the following tasks should be completed
  - Verify basic configuration and router operations.
  - Save the changes on a router

Configuration - verification

Verify Basic Router/Switch Configuration

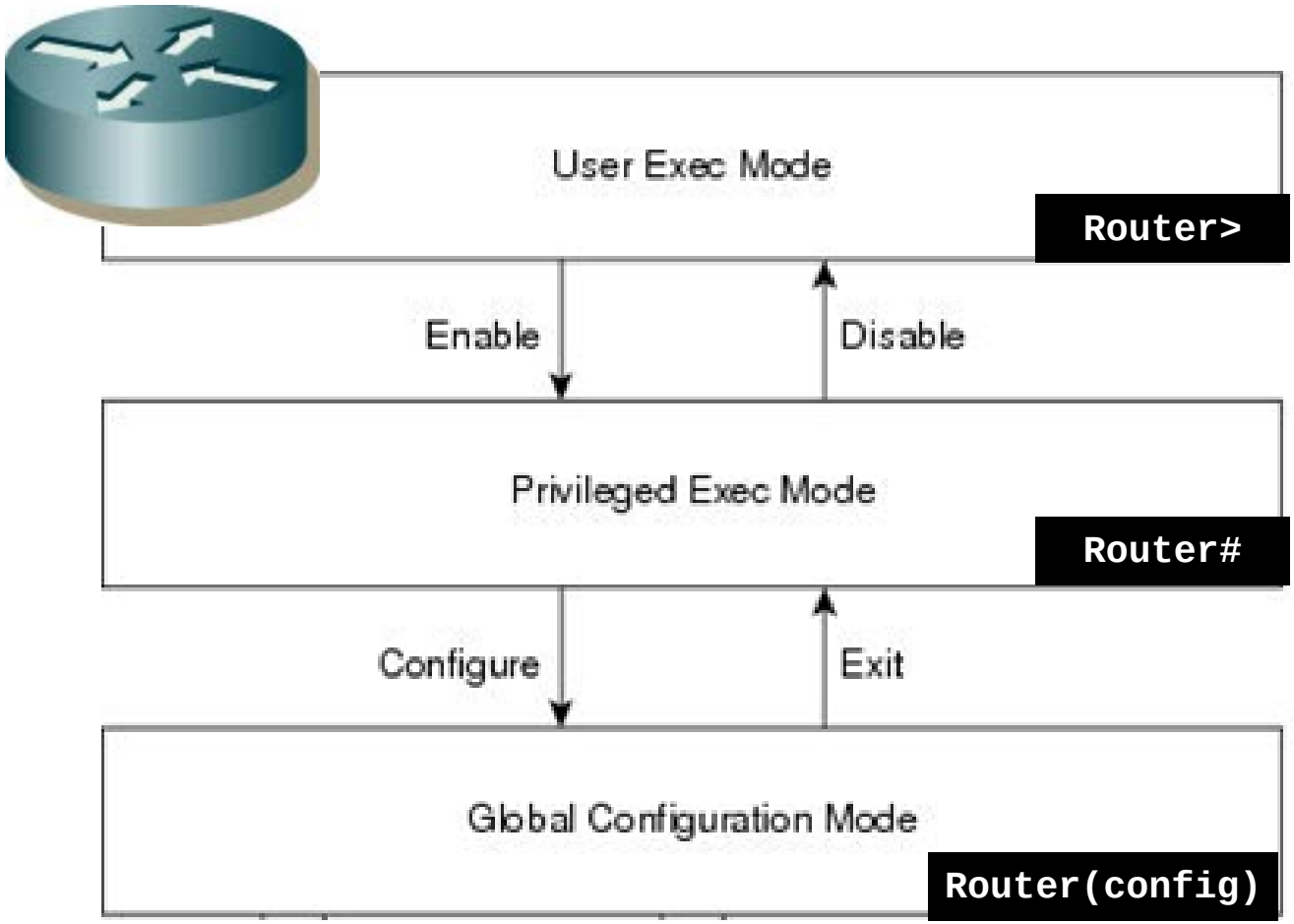
Issue the *show running-config* command

Save the basic router configuration by Issuing the *copy running-config startup-config* command

Additional commands that will enable you to further verify router configuration are:

- Show running-config - Displays configuration currently in RAM
- Show startup-config - Displays configuration file NVRAM
- Show IP route - Displays routing table
- Show interfaces - Displays all interface configurations
- Show IP interface brief - Displays abbreviated interface configuration information

Cisco Device Command Modes



Changing prompt mode

Cisco IOS CLI Command Syntax	
Switch from user EXEC to privileged EXEC mode.	`switch>enable`
If a password has been set for privileged EXEC mode you will be prompted to enter it now.	`Password:password`
The # prompt signifies privileged EXEC mode.	`switch#`
Switch from privileged EXEC to user EXEC mode.	`switch#disable`
The > prompt signifies user EXEC mode.	`switch>`

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`switch#configure terminal`
The (config)# prompt signifies that the switch is in global configuration mode.	`switch(config)#`
Switch from global configuration mode to interface configuration mode for fast ethernet interface 0/1.	`switch(config)#interface fastethernet 0/1`
The (config-if)# prompt signifies that the switch is in the interface configuration mode.	`switch(config-if)#`
Switch from interface configuration mode to global configuration mode.	`switch(config-if)#exit`
The (config)# prompt signifies that the switch is in global configuration mode.	`switch(config)#`
Switch from global configuration mode to privileged EXEC mode.	`switch(config)#exit`
The # prompt signifies that the switch is in privileged EXEC mode.	`switch#`

Error notification

Example Error Message	Meaning	How to Get Help
switch#**cl** % Ambiguous command: "cl"	You did not enter enough characters for your device to recognize the command.	Re-enter the command followed by a question mark (?), without a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
switch#**clock** % Incomplete command.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?), with a space between the command and the question mark.
switch#**clock set aa:12:23** ^ % Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands or parameters that are available.

Basic Router Configuration Command Syntax

Naming the router	`Router(config)#hostname name`
Setting Passwords	`Router(config)#enable secret password`
	`Router(config)#line console 0`
	`Router(config-line)#password password`
	`Router(config-line)#login`
	`Router(config)#line vty 0 4`
	`Router(config-line)#password password`
	`Router(config-line)#login`
Configuring a message-of-the-day banner	`Router(config)#banner motd # message #`

Basic Router Configuration Command Syntax

Configuring an interface	`Router(config)#interface type number`
	`Router(config-if)#ip address address mask`
	`Router(config-if)#description description`
	`Router(config-if)#no shutdown`
Saving changes on a router	`Router#copy running-config startup-config`
Examining the output of **show** commands	`Router#show running-config`
	`Router#show ip route`
	`Router#show ip interface brief`
	`Router#show interfaces`