

آزمایشگاه شبکه های کامپیوتری

جلسه اول

گردآورنده: زهرا کریمی

مفاهیم پایه

► شبکه کامپیوتری چیست؟

► به مجموعه ای از تجهیزات (Devices) به هم مرتبط گفته می شود که توانایی تبادل داده و اطلاعات را با یکدیگر داشته باشند.

► به اعضای شبکه در اصطلاح گره (node) یا میزبان (host) گفته می شود.

► اهداف شبکه

► به اشتراک گذاشتن منابع: (سخت افزاری - نرم افزاری)

► ایجاد ارتباط: (پست الکترونیک، چت، کنفرانس های ویدئویی، تلفن های اینترنتی و ...)

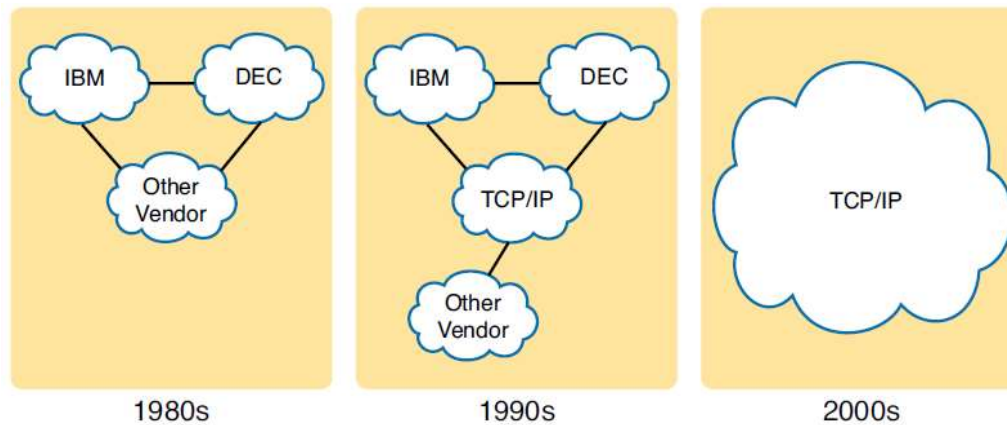
The networks' job is simply this:

Moving data from one device to another.

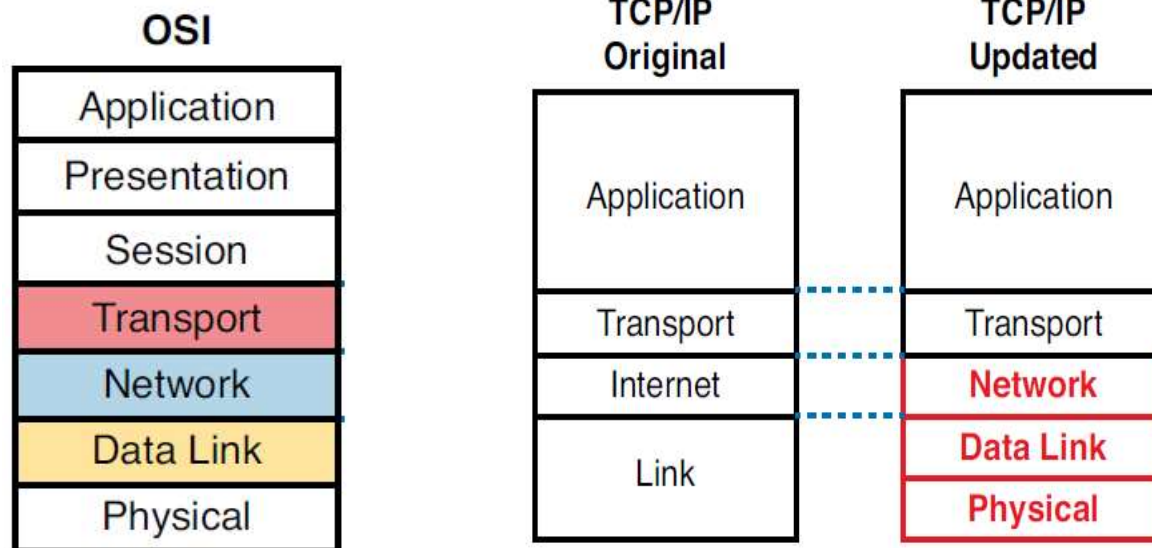
مدل های شبکه

► مدل شبکه (Networking Model)

مجموعه قوانین و رول هایی هستند که مشخص می کنند هر قسمت از شبکه به صورت جداگانه چگونه باید کار کنند و همچنین کل قسمت ها چگونه با هم ارتباط برقرار کنند تا کل شبکه به صورت صحیح فعالیت نماید.



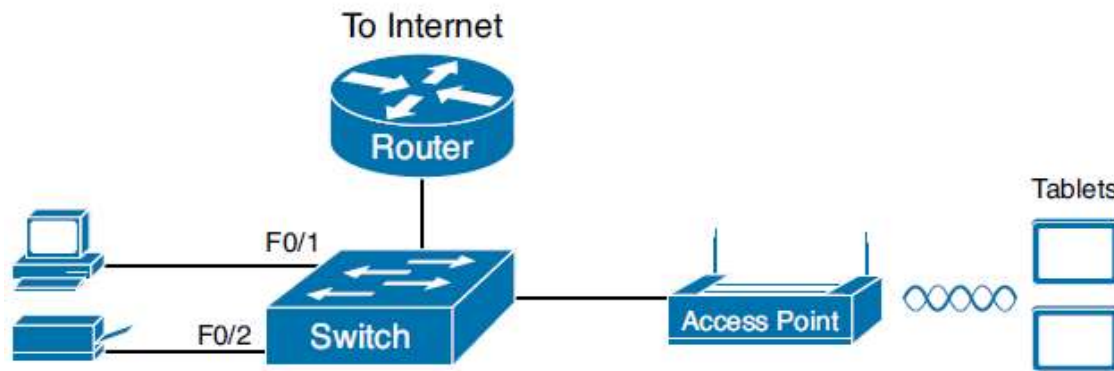
بررسی اجمالی مدل های شبکه TCP/IP و OSI



Two TCP/IP Networking Models

پایه و اساس Ethernet Lans

- ▶ بیشتر شبکه های کامپیوتری اینترپرایز امروزی بر پایه دو تکنولوژی به نام های LAN و WAN شکل گرفته اند.
- ▶ امروزه شبکه ها از دو نوع Lan به نام های Ethernet Lan و Wireless Lan استفاده می کنند.



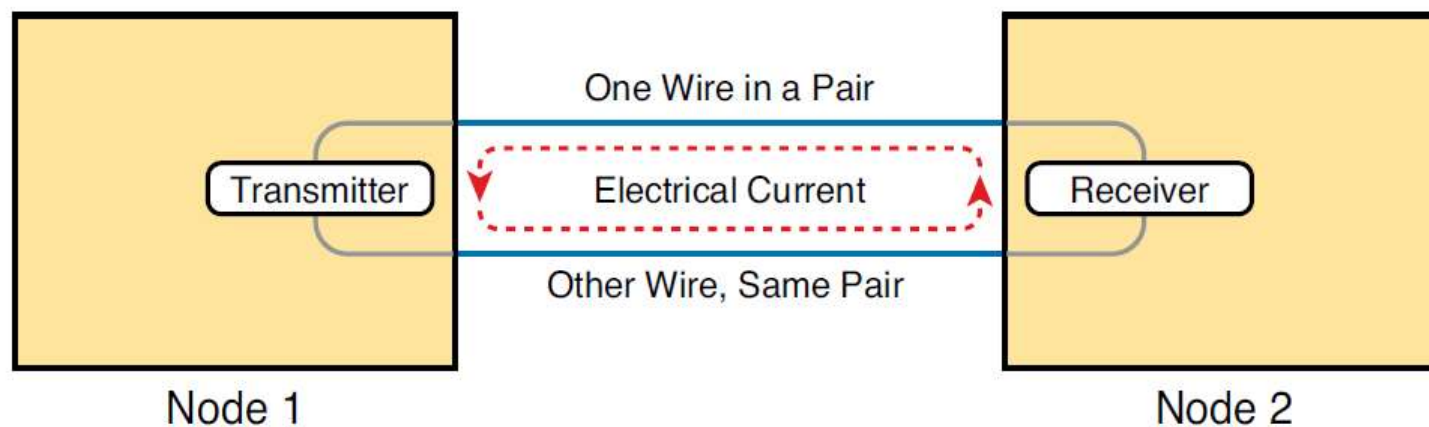
Typical Small Wired and Wireless SOHO LAN

انواع استانداردهای لایه فیزیکی اترنت

Examples of Types of Ethernet

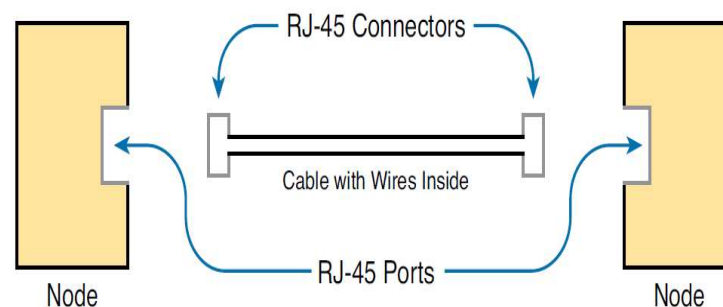
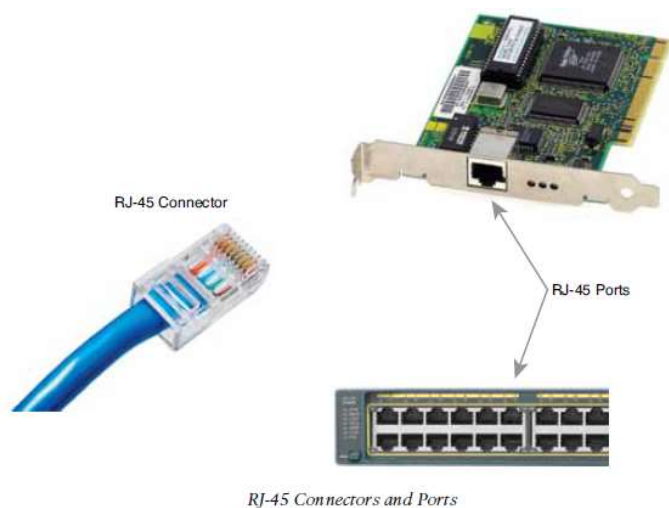
Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

انتقال داده با استفاده از کابل های Twisted Pairs



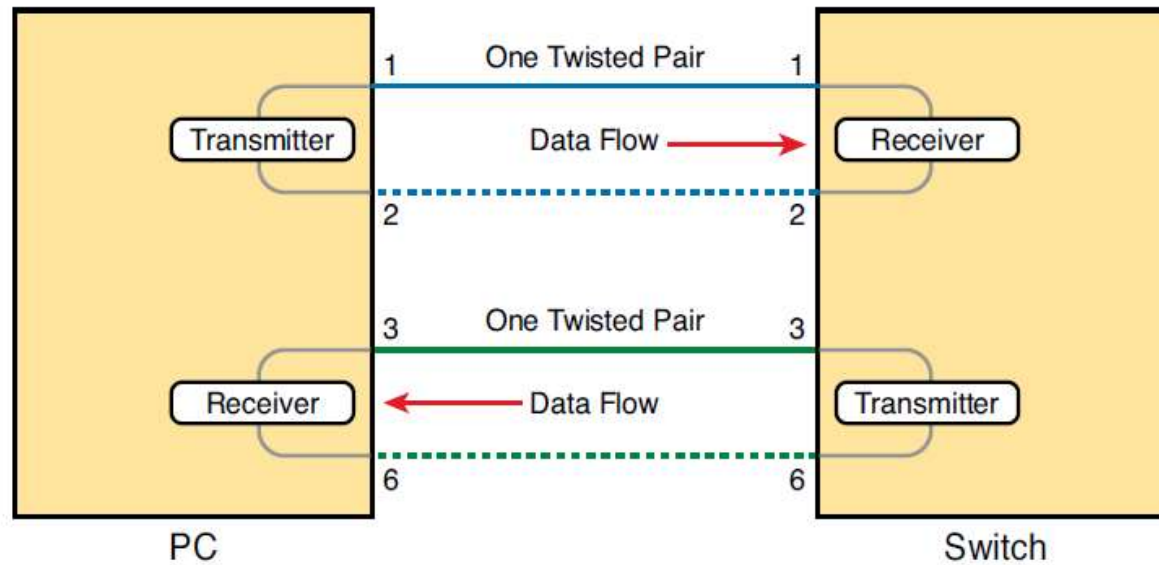
Creating One Electrical Circuit over One Pair to Send in One Direction

انتقال داده با استفاده از کابل های Twisted Pairs



Basic Components of an Ethernet Link

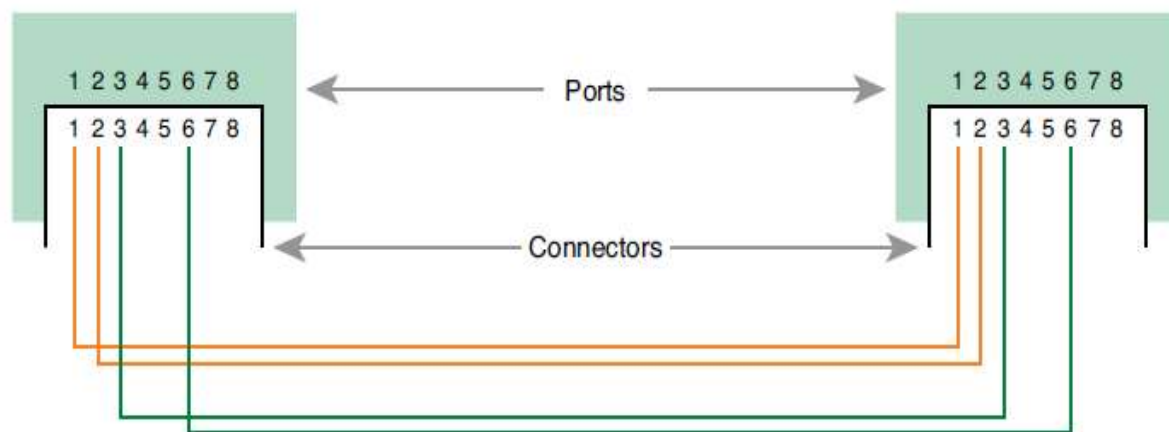
انتقال داده با استفاده از کابل های Twisted Pairs



Using One Pair for Each Transmission Direction with 10- and 100-Mbps Ethernet

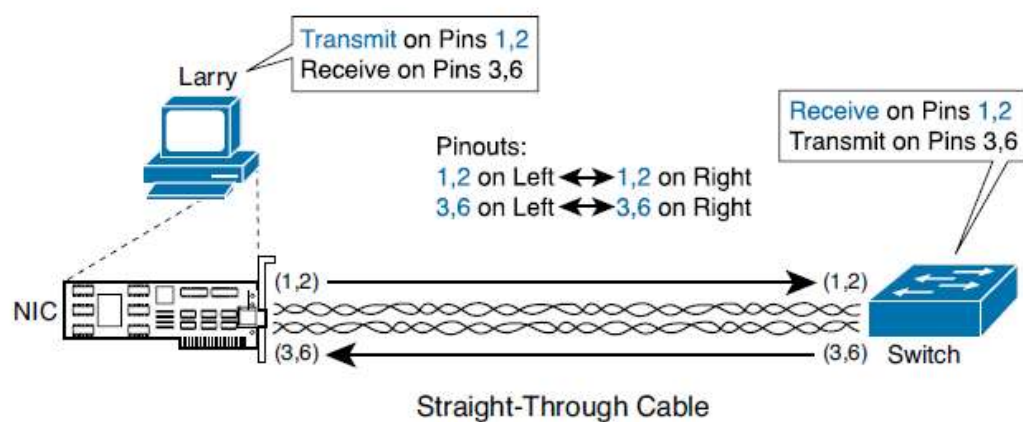
انواع کابل ها از لحاظ چیدمان سیم ها

Straight through Cables ►



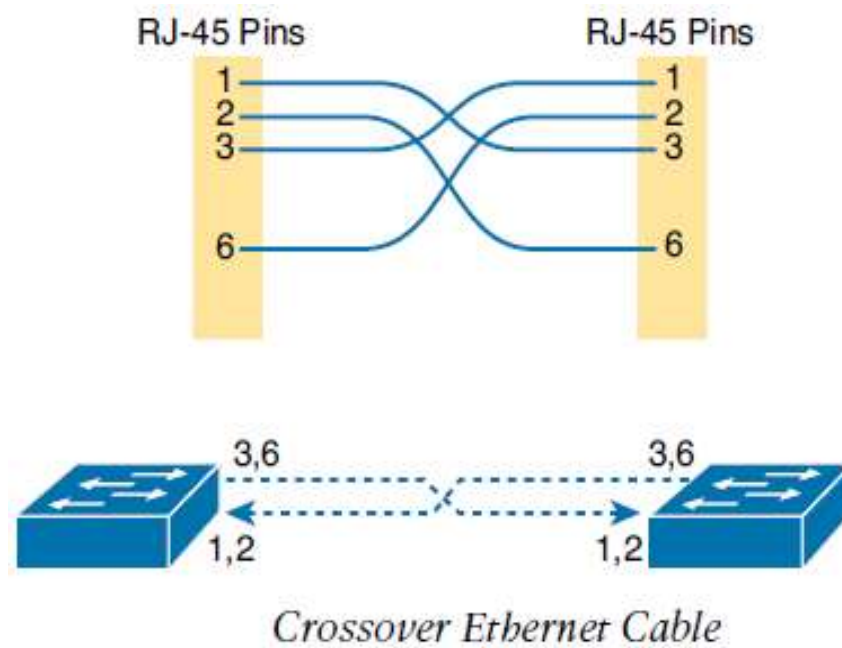
10BASE-T and 100BASE-T Straight-Through Cable Pinout

مفهوم ارسال از طریق کابل Straight through Cable



Ethernet Straight-Through Cable Concept

مفهوم ارسال از طریق کابل Crossover Cable

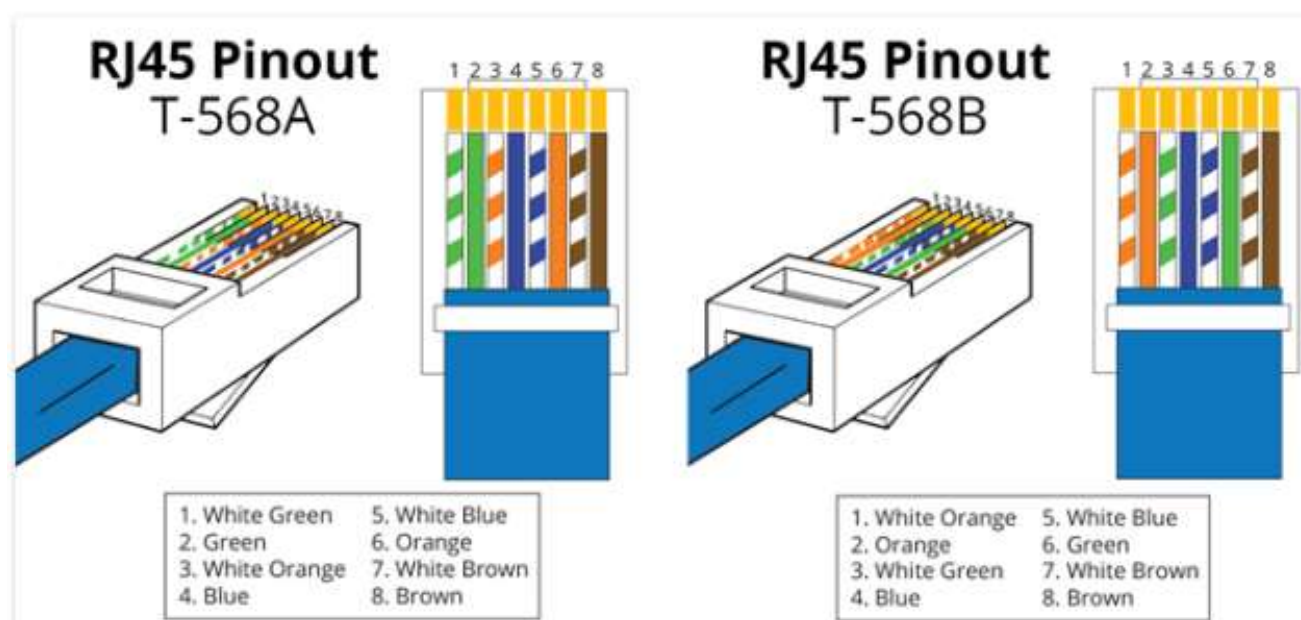


انتخاب صحیح چیدمان کابل ها

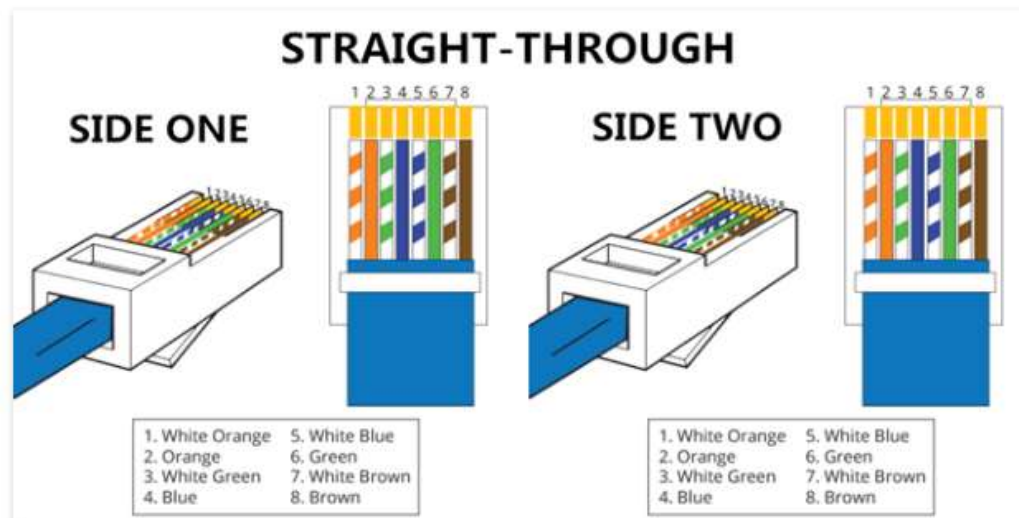
10BASE-T and 100BASE-TX Pin Pairs Used

Transmits on Pins 1,2	Transmits on Pins 3,6
PC NICs	Hubs
Routers	Switches
Wireless access point (Ethernet interface)	—

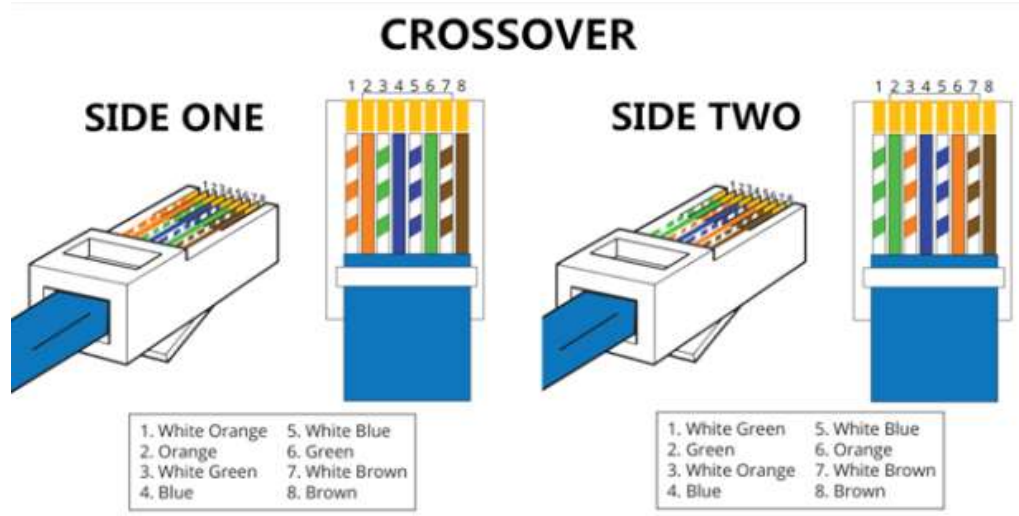
آشنایی با ترتیب رنگ بندی در دو استاندارد A و B



Straight Through cable Pin



Crossover Cable Pinout



آزمایشگاه شبکه های کامپیوتری

جلسه دوم

(TCP/IP Addressing)

گردآورنده: زهرا کریمی

مفاهیم آدرس دهی (TCP/IP Addressing)

- What is an IP Address?
- Ex: 192 . 168 . 1 . 15 (Dotted-Decimal Notation=DDN)
 └─┘ └─┘ └─┘ └─┘
 octet octet octet octet
- octet = 8 bit
- IP Add = 4*8=32 bit

Values Associated with Each Bit in an Octet

Bit	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1

Calculating the Decimal Value of 192 in Binary

Bit	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1
State	On	On						

مفاهیم آدرس دهی (TCP/IP Addressing)

- ▶ How to show IP Address?
- ▶ subnet mask format

IP: 192.168..1.2
Subnet mask: 255.255.255.0

- ▶ prefix format

192.168.1.2/24

Subnet MASK

- ▶ Subnet Mask job: divide an IP Address into 2 parts,
- ▶ Net ID and Host Id

Identifying the Network ID and Host ID Portions of an IP Address

	Octet 1	Octet 2	Octet 3	Octet 4
IP address	192	168	1	15
Subnet mask	255	255	255	0
Address portion	N	N	N	H

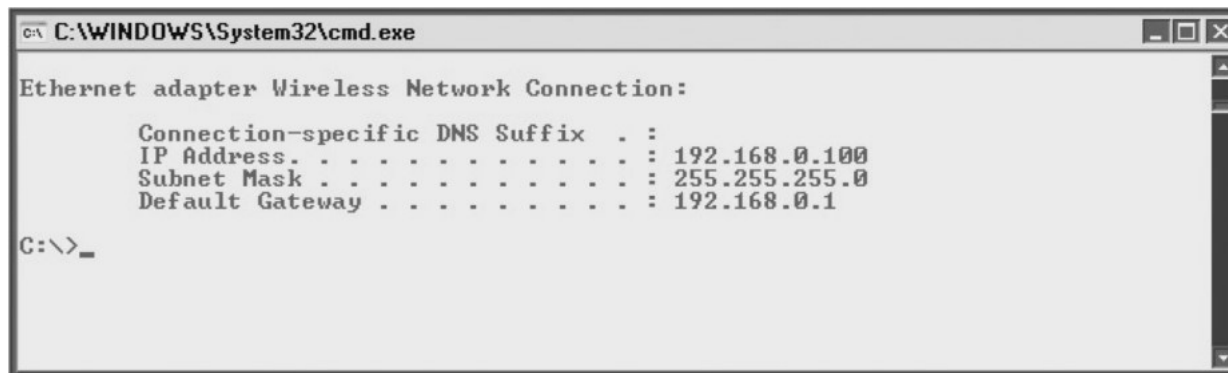
Subnet MASK

► Identifying Remote Systems

ComputerA (IP address)	ComputerA (Subnet mask)	ComputerB (IP address)	Same Network?
12.45.8.34	255.0.0.0	14.34.212.5	
131.107.4.78	255.255.0.0	131.108.45.112	
198.45.23.2	255.255.255.0	198.45.23.14	
26.45.78.5	255.0.0.0	28.45.78.15	
176.34.56.12	255.255.0.0	176.34.12.10	

Default gateway

- Send data to another network by using Default gateway



```
C:\WINDOWS\System32\cmd.exe

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

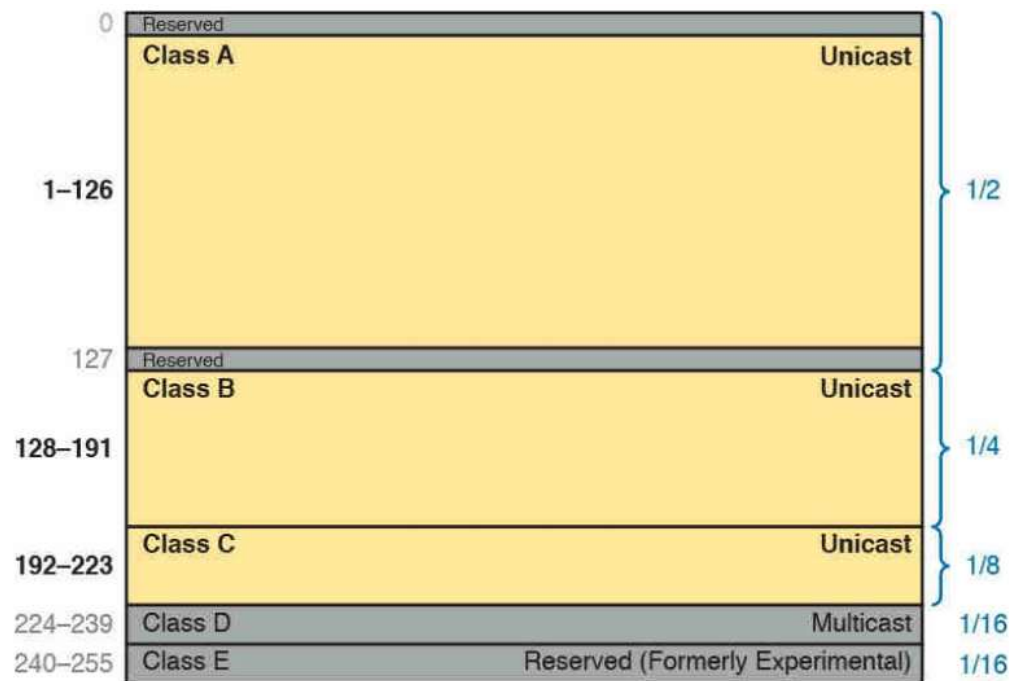
C:\>_
```

Address Classes

- ▶ Every IP address belongs to a distinct address class
- ▶ Class A (Default subnet mask 255.0.0.0)
- ▶ Class B (Default subnet mask 255.255.0.0)
- ▶ Class C (Default subnet mask 255.255.255.0)
- ▶ Class D (Used by multicasting application)
- ▶ Class E (Used for experimental purposes)

Address Classes

- Every IP address belongs to a distinct address class



Division of the Entire IPv4 Address Space by Class

Loopback Address

- ▶ is used to refer to the local system (localhost)
- ▶ To verify that TCP/IP protocol stack is functioning on your local system
- ▶ Ping loopback address 127.0.0.1

Private and Public Address

- ▶ **Private addresses:** are nonroutable addresses (can be assigned to a system without Internet connectivity)
 - ▶ 10.0.0.0 – 10.255.255.255 (Class A)
 - ▶ 172.16.0.0 – 172.31.255.255 (Class B)
 - ▶ 192.168.0.0 – 192.168.255.255 (Class C)
- ▶ **Public Addresses :** are routable addresses (with Internet connectivity)
 - ▶ All Class A, B and C except Private addresses

Valid and Illegal Address

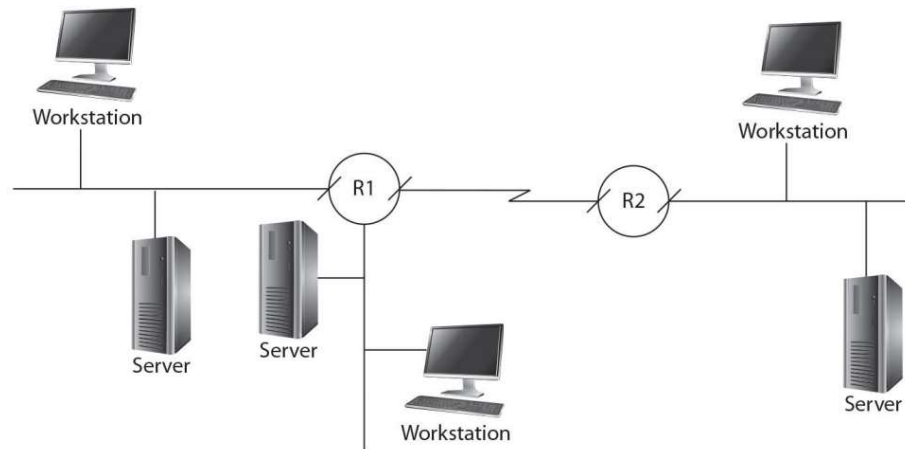
- ▶ **Illegal addresses:** cannot be assigned to hosts
 - ▶ Any address starting with 127
 - ▶ All host bits set to 0 (Network Address)
 - ▶ All host bits set to 1 (Broadcast Address)
 - ▶ A Duplicate address
- ▶ **Valid Address:** can be assigned to hosts

Addressing Schemes

- ▶ Unicast: sending information to 1 system
- ▶ Broadcast: sending information to all systems
- ▶ Multicast: sending information to a selected group of systems

Subnetting

- ▶ Take one address range and break it down into multiple address range
- ▶ Can assign each address range to a separate network (subnet)
 - ▶ Due to physical location
 - ▶ Reduce traffic
 - ▶ Security issues



Understanding Subnetting

- ▶ Takes some of the host bits from the subnet mask and uses them as additional network bits by setting the bits to a “1”
- ▶ This creates additional networks, but results in fewer hosts on the network
- ▶ How many host bits?
 - ▶ $2^{\text{Masked bits}} \geq \text{Number of Subnets}$

Example of Subnetting

- ▶ IP range 10.0.0.0/8
- ▶ # of subnets = 4
- ▶ How many host bits : 2 ($2^2 = 4$)

Decimal	255	0	0	0
Binary	11111111	00000000	00000000	00000000

Old subnet mask:255.0.0.0

Decimal	255	192	0	0
Binary	11111111	11000000	00000000	00000000

New subnet mask:255.192.0.0

Example of Subnetting

- **New subnet mask** After subnetting a network, you will have a new subnet mask that is used by all subnets you have created.
- **Network ID** All host bits are set to 0.
- **First valid address** The least significant host bit is set to 1; all other host bits are 0.
- **Broadcast address** All host bits are set to 1.
- **Last valid address** The least significant host bit is set to 0; all other host bits are 1.

Example of Subnetting

	First Octet (Decimal)	Second Octet (Binary)	Third Octet (Binary)	Fourth Octet (Binary)
Original IP	10	0	0	0
	10	00000000	00000000	00000000
	10	01000000	00000000	00000000
	10	10000000	00000000	00000000
	10	11000000	00000000	00000000



Interested octet

Example of Subnetting

Calculate New Network IDs

	First Octet (Decimal)	Second Octet (Binary)	Third Octet (Binary)	Fourth Octet (Binary)	Calculation
Original IP	10	0	0	0	
Subnet #1	10	00000000	00000000	00000000	10.0.0.0
Subnet #2	10	01000000	00000000	00000000	10.64.0.0
Subnet #3	10	10000000	00000000	00000000	10.128.0.0
Subnet #4	10	11000000	00000000	00000000	10.192.0.0

Example of Subnetting

Calculate First IP Address

	First Octet (Decimal)	Second Octet (Binary)	Third Octet (Binary)	Fourth Octet (Binary)	Calculation
Original IP	10	0	0	0	
Subnet #1	10	00000000	00000000	00000001	10.0.0.1
Subnet #2	10	01000000	00000000	00000001	10.64.0.1
Subnet #3	10	10000000	00000000	00000001	10.128.0.1
Subnet #4	10	11000000	00000000	00000001	10.192.0.1

Example of Subnetting

Calculate Broadcast IP Address

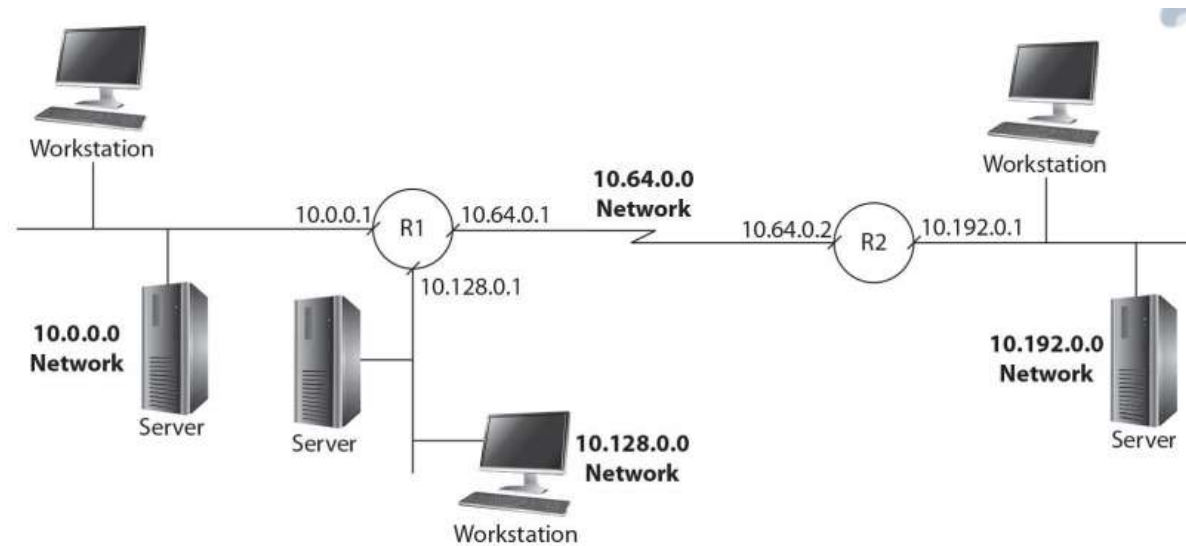
	First Octet (Decimal)	Second Octet (Binary)	Third Octet (Binary)	Fourth Octet (Binary)	Calculation
Original IP	10	0	0	0	
Subnet #1	10	00111111	11111111	11111111	10.63.255.255
Subnet #2	10	01111111	11111111	11111111	10.127.255.255
Subnet #3	10	10111111	11111111	11111111	10.191.255.255
Subnet #4	10	11111111	11111111	11111111	10.255.255.255

Example of Subnetting

Calculate Last IP Address

	First Octet (Decimal)	Second Octet (Binary)	Third Octet (Binary)	Fourth Octet (Binary)	Calculation
Original IP	10	0	0	0	
Subnet #1	10	00111111	11111111	11111110	10.63.255.254
Subnet #2	10	01111111	11111111	11111110	10.127.255.254
Subnet #3	10	10111111	11111111	11111110	10.191.255.254
Subnet #4	10	11111111	11111111	11111110	10.255.255.254

Example of Subnetting



	Network ID	First Valid Address	Last Valid Address	Broadcast Address	Subnet Mask
Subnet 1	10.0.0.0	10.0.0.1	10.63.255.254	10.63.255.255	255.192.0.0
Subnet 2	10.64.0.0	10.64.0.1	10.127.255.254	10.127.255.255	255.192.0.0
Subnet 3	10.128.0.0	10.128.0.1	10.191.255.254	10.191.255.255	255.192.0.0
Subnet 4	10.192.0.0	10.192.0.1	10.255.255.254	10.255.255.255	255.192.0.0

آزمایشگاه شبکه های کامپیوتری

جلسه سوم

TCP/IP Utilities

&

Troubleshooting

گردآورنده: زهرا کریمی

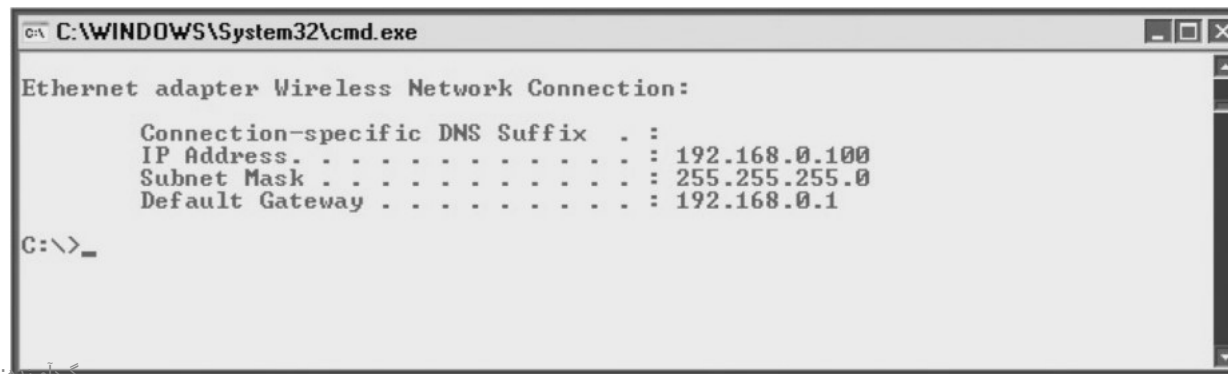
آشنایی با کارت شبکه (NIC: Network Interface Card)

- ▶ چک کردن چراغ های روی کارت شبکه
- ▶ اطمینان از نصب درایور مناسب کارت شبکه
- ▶ اطمینان از برقراری ارتباط کابل
- ▶ اطمینان از برقراری ارتباط بی سیم با اکسس پوینت
- ▶ چک کردن سرعت انتقال داده بر روی کارت شبکه
- ▶ چک کردن آدرس IP مربوط به کارت شبکه

- ▶ Windows: ipconfig
- ▶ Linux: ifconfig

آشنایی با دستورات ipconfig/ifconfig

- ▶ Windows :ipconfig /all
- ▶ Linux: ifconfig



```
C:\WINDOWS\System32\cmd.exe

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\>_
```

آشنایی با دستور Ping

- ▶ Ping : Packet Internet Groper
- ▶ Ping uses Internet Control Message Protocol(ICMP)
- ▶ Ping <target>
- ▶ ttl : Time To Live
- ▶ rtt : Round Trip Time

```
C:\Users\admin>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

آشنایی با دستور arp

- ▶ Arp : Address Resolution protocol
- ▶ Usage: changing Mac address to IP address
- ▶ What is Mac Address?
- ▶ Mac: Media Access control (48 bit)
- ▶ Windows: arp -a
- ▶ Windows: arp -s <IP add> <mac add>
- ▶ Windows: arp -d <IP add>
- ▶ Linux: arp -n

آزمایشگاه شبکه های کامپیوتری

جلسه چهارم

TCP/IP Utilities & Troubleshooting

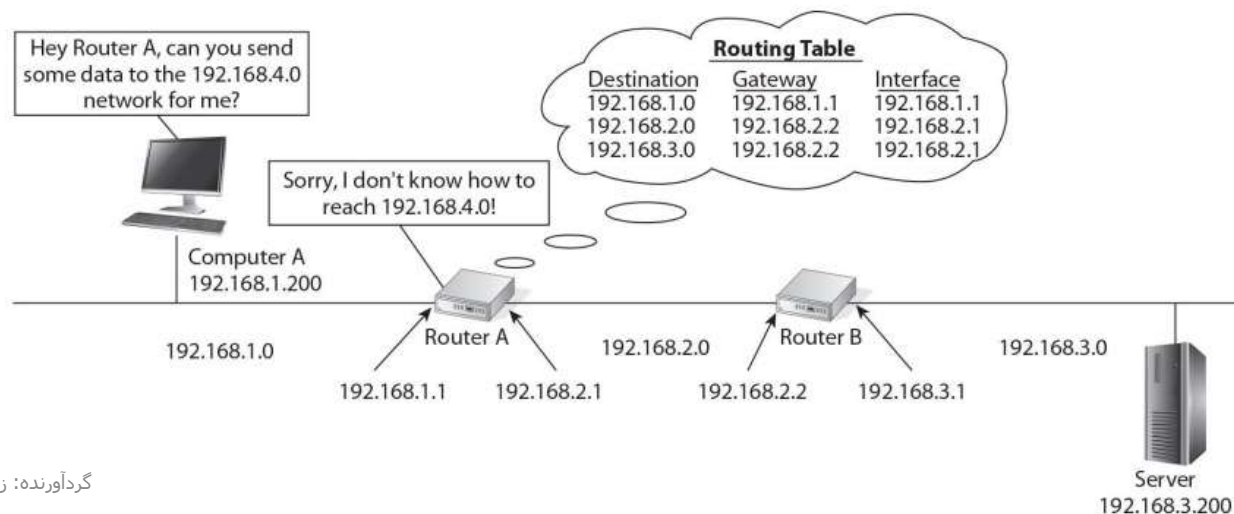
گردآورنده: زهرا کریمی

آشنایی با دستور Traceroute

- ▶ Determine the path taken by a data packet to reach its destination.
 - ▶ Tracert will send you a response with each router that is hit on the way
 - ▶ Use **ICMP** as their underlying protocol
-
- ▶ Windowd: `tracert <hostname|ipaddress>`
 - ▶ Linux: `traceroute <hostname|ipaddress>`

آشنایی با دستور route

- ▶ *Routing* involves sending data from one network to another
- ▶ The router is responsible for routing information to the destination network
- ▶ Route is used to manage the routing table of the local system



آشنایی با دستور route

► Routing Concepts

- **Loopback interface:** is a virtual network interface card configured on the router
- **Routing loops:** is when you have two routers sending the packet back and forth to one another
- **Routing tables :**is used to determine where the router needs to send a packet when it reaches the router
- **Static vs. dynamic routes;** Routes are either manually added to a routing table or they are automatically learned from other routers
- **Default route:** will be used if there is no entry in the routing table that matches the destination IP address of the packet

آشنایی با دستور route

► windows:

- route print
- route delete <Destination route>
- route add <Destination IP> MASK <subnet mask>
<next_hop>

► Linux:

- route -n
- route add -net <network_id> netmask <mask> gw
<gateway_ip>
- route del -net <network_id> netmask <mask> gw
<gateway_ip>

آزمایشگاه شبکه های کامپیوتری

جلسه پنجم

TCP/IP Utilities

&

Troubleshooting

گردآورنده: زهرا کریمی

DNS Servers

- ▶ DNS is a network service that is responsible for converting fully qualified domain names (FQDNs) to IP addresses
- ▶ DNS has a hierarchical structure that allows it to support networks of any size
 - ▶ www.yahoo.com
 - ▶ 87.248.98.8

DNS Servers hierarchy

- ▶ **Root Servers:** forward the request to the name servers at the next level down
- ▶ **Top Level Domains(TLD):** is one of the domains at the highest level in the hierarchical Domain Name System
 - ▶ .com, .org, .net, .edu, .gov, .mil, .int
- ▶ **Second Level Domains(SLD or 2LD):** is a domain that is directly below a top-level domain

DNS Servers Zone

- ▶ DNS Zone: is the area of the dns hierarchy that you are responsible for managing
- ▶ Primary DNS Zone: is a read/write copy of the zone data & is where you create the DNS records
- ▶ Secondary DNS Zone: is a read-only copy of the dns data to have a backup

Types of DNS Records

- ▶ Host(A)
- ▶ Host(AAAA)
- ▶ Alias(cname)
- ▶ Mail Exchange(MX)
- ▶ Name Server(NS)
- ▶ Start of Authority(SOA)
- ▶ Pointer(ptr)

آشنایی با دستور nslookup

► Interactive mode

- nslookup
- server<new dns server ip address>
- hostname
- set type=<record type> OR set q=<record type>

► Noninteractive mode

- nslookup <hostname>

آشنایی با دستور dig و host در لینوکس

- ▶ `dig [@ server] -t <record type> <hostname> [+short]`
- ▶ `host -t <record type> <hostname> [server]`

آزمایشگاه شبکه های کامپیوتری

جلسه ششم

TCP/IP Utilities

&

Troubleshooting

گردآورنده: زهرا کریمی

TCP Ports

- ▶ TCP port is an identifier for applications
- ▶ There are 3 types of ports:
 - ▶ Well-known ports: are used by servers(0-1023)
 - ▶ Registered ports: are used by certain applications(1024-49151)
 - ▶ Dynamic ports: are used by applications temporarily(49152-65535)

TCP Ports

Ports Used by Popular Internet Applications

Port Number	Process	Description
20	FTP-DATA	File Transfer Protocol—used to transfer data from one machine to another
21	FTP	File Transfer Protocol—used for control messages of the FTP session
22	SSH	Secure Shell
23	TELNET	Telnet—used to create a terminal session
25	SMTP	Simple Mail Transfer Protocol—used to send e-mail across the Internet
53	DNS	Domain Name System—used to query DNS servers for the IP address of a remote system
67,68	DHCP	Used by Domain Host Configuration Protocol (DHCP) clients and servers to automatically configure clients
69	TFTP	Trivial File Transfer Protocol
80	HTTP	Hypertext Transfer Protocol—used to deliver webpages from a web server to the web client
110	POP3	Post Office Protocol, version 3—a protocol for reading e-mail over the Internet
119	NNTP	Network News Transfer Protocol—used to read news articles from a news server
123	NTP	Network Time Protocol—used to synchronize the time on systems

کردآورنده: زهرا کریمی

آشنایی با دستور Netstat

- ▶ A Swiss Army Knife
- ▶ Displaying server connections & listening ports
- ▶ Displaying interface statistics
- ▶ Displaying per-protocol statistics
- ▶ Displaying the current routing table



آشنایی با دستور netstat در ویندوز

- ▶ netstat -n: displaying addresses and port numbers in numerical form
- ▶ netstat -a: Displays all connections and listening ports
- ▶ netstat -e: displaying interface statistics
- ▶ netstat -s: displaying per-protocol statistics
- ▶ netstat -p <protocol> : displaying per-protocol connections
- ▶ netstat -r : displaying the routing table

آشنایی با دستور netstat در لینوکس

- ▶ netstat -r: display routing table
- ▶ netstat -s: display networking statistics
- ▶ netstat -n: don't resolve names
- ▶ netstat -e: display other/more information
- ▶ netstat -p: display PID/Program name
- ▶ netstat -c: continuous listing
- ▶ netstat -l: display listening server connections
- ▶ netstat -a: display all connections (default: connected)

آشنایی با دستور nmap در لینوکس

- ▶ Nmap(Network Mapper) is an open source Linux command line tool for network exploration and security auditing
- ▶ Nmap uses raw IP packets in novel ways to determine what hosts are available on the network
- ▶ what services (application name and version) those hosts are offering
- ▶ what operating systems (and OS versions) they are running
- ▶ what type of packet filters/firewalls are in use
- ▶ And ...

آشنایی با دستور nmap در لینوکس

- ▶ -sL: List Scan - simply list targets to scan
- ▶ -sn: Ping Scan - disable port scan
- ▶ -sT: Stealth TCP Scan
- ▶ -sS: Stealth TCP Scan
- ▶ -sU: UDP Scan
- ▶ -p <port ranges>: Only scan specified ports
 - ▶ Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
- ▶ -F: Fast mode - Scan fewer ports than the default scan
- ▶ -sV: Probe open ports to determine service/version info
- ▶ -O: Enable OS detection
- ▶ -V: Print version number
- ▶ -A: Enable OS detection, version detection, script scanning, and traceroute

گذاورن به هر کاری

آزمایشگاه شبکه های کامپیوتری

جلسه هفتم

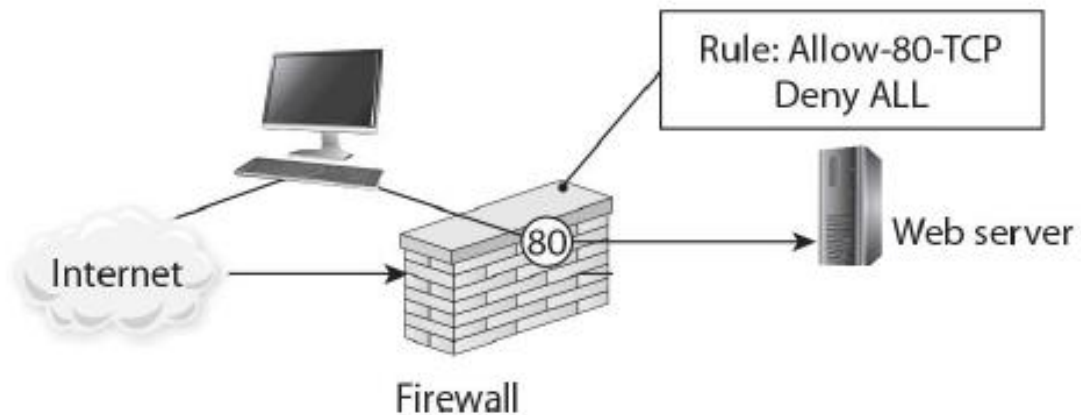
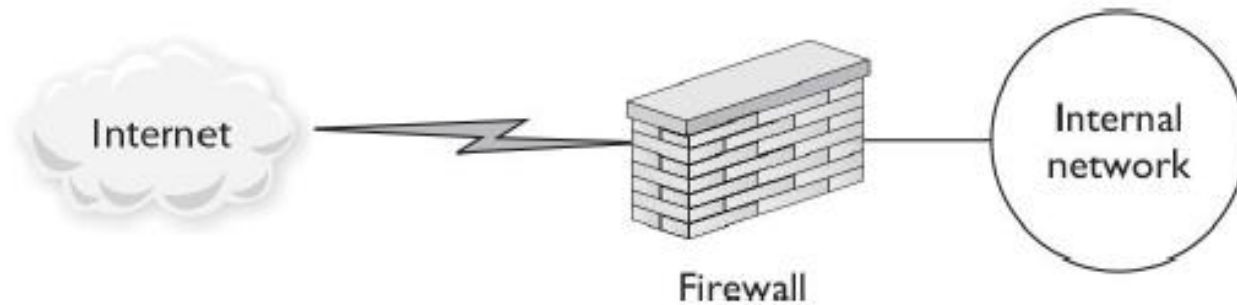
Firewall

گردآورنده: زهرا کریمی

آشنایی با سرویس Firewall

- ▶ Firewalls are a networking component responsible for protecting the network from outside intruders.
- ▶ Firewalls on routers can be used to create rules that control communication from different parts of the network.
- ▶ Firewalls can be either software-based solutions or hardware device
- ▶ You configure rules on the firewall that indicate which traffic is to pass through and which is to be blocked

آشنایی با سرویس Firewall

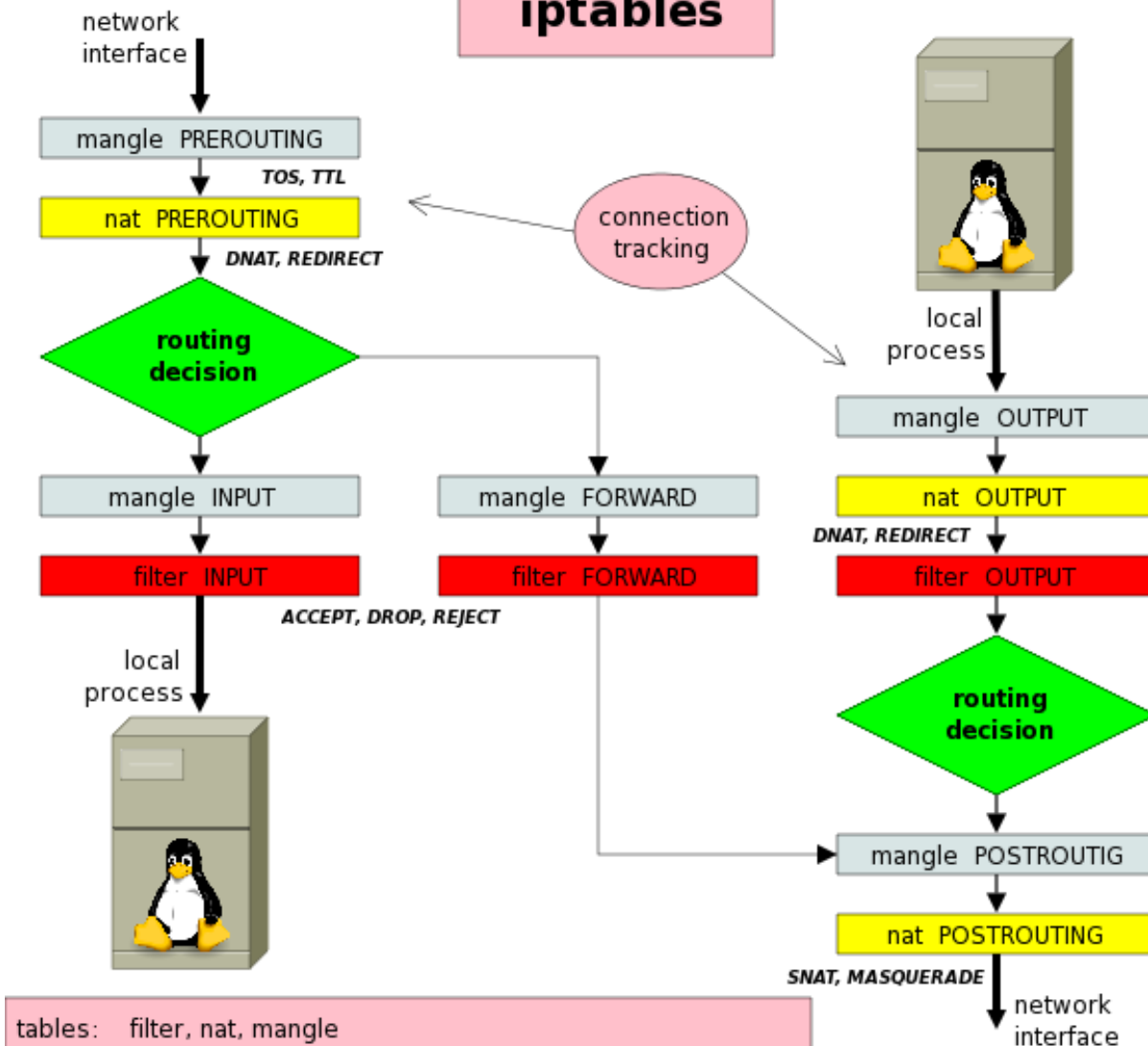


ساختار iptable

► iptables consists of :

table	chain
filter	INPUT OUTPUT FORWARD
nat	PREROUTING POSTROUTING OUTPUT
mangle	PREROUTING INPUT FORWARD OUTPUT POSTROUTING

iptables



tables: filter, nat, mangle
 chains: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING
 targets: ACCEPT, DROP, REJECT, DNAT, SNAT, MASQUERADE, REDIRECT, LOG, RETURN, TTL, TOS, ...

ساختار هر rule

- ▶ iptables [options] [chain] -j [target]
- ▶ --append -A chain (Append to chain)
- ▶ --delete -D chain (Delete matching rule from chain)
- ▶ --delete -D chain rulenum (Delete rule rulenum (1 = first) from chain)
- ▶ --insert -I chain [rulenum] (Insert in chain as rulenum (default 1=first))
- ▶ --flush -F [chain] (Delete all rules in chain or all chains)
- ▶ --list -L [chain [rulenum]] (List the rules in a chain or all chains)
- ▶ --source -s address[/mask][...] (source specification)
- ▶ --destination -d address[/mask][...] (destination specification)
- ▶ --table -t table (table to manipulate: filter, nat, mangle (default: 'filter'))
- ▶ --jump -j target (target for rule: ACCEPT, DROP, REJECT)