Fundamentals of Computer Networking

Fundamentals of Computer Networking

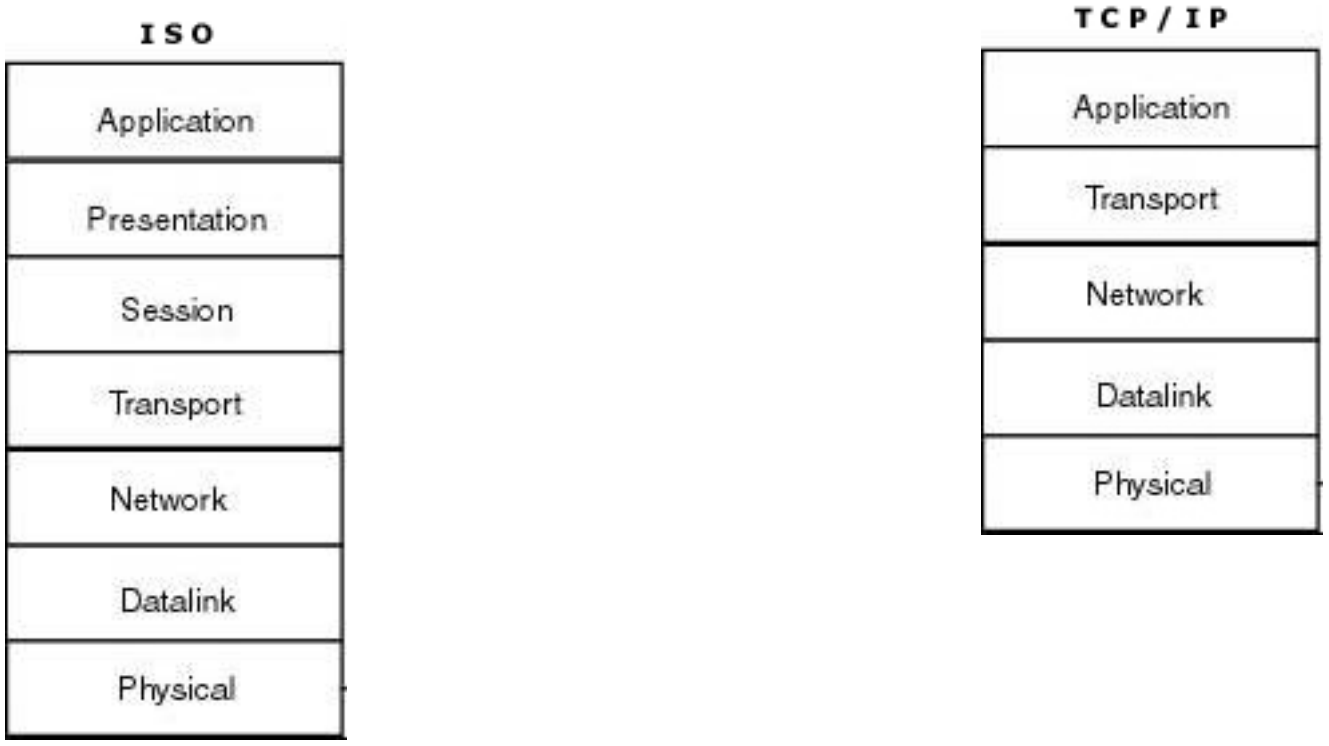
- Computer networks are an integral part of the modern computing infrastructure
- The local network (LAN) is usually Ethernet
- LAN's are inter-connected with other LAN's in a hierarchical fashion eventually forming the Internet

Fundamentals of Computer Networking

- The operation of computer networks is governed by hardware and software protocols
- There are two standard network models
  - The 7-layer ISO model
    http://en.wikipedia.org/wiki/OSI_model
  - The 5-layer TCP/IP model
    http://en.wikipedia.org/wiki/TCP/IP_model
- These models are abstract representations of the division of labor

Fundamentals of Computer Networking

Network Models



Network Model

- Layer 1 (Physical) is the electrical specification
- Layer 2 (Data Link) defines the interface to Layer 1
- Layer 3 (Network) is generally responsible for transferring data between networks
- Layer 4 (Transport) is generally responsible for packaging data into packets for transfer between computers
- Layer 5 (Application) is generally responsible for communication between applications

Ethernet

- The networking protocol of the Local Area Network is Ethernet http://en.wikipedia.org/wiki/Ethernet
- Ethernet is defined in layers 1 and 2

TCP/IP Suite

- The networking protocol of the Internet is TCP/IP
http://en.wikipedia.org/wiki/TCP/IP

- The functionality of TCP/IP resides in layers 3, 4, and 5

Layer 2 - Ethernet

- Ethernet was invented by Xerox in 1970's
- Speeds are currently 10, 100, 1000 Mbps
- Data is packaged in frames
- The major contents of a frame are
  - source address (6 bytes)
  - destination address (6 bytes)
  - payload (up to 1500 bytes)

Layer 2 - Ethernet

- An ethernet is 48 bits in length and each device has a unique address
- An ethernet address is usually referred to by the terms
  - MAC address
  - Physical address
- The address is normally written as
  - xx:xx:xx:xx:xx:xx
  - xx-xx-xx-xx-xx-xx
  - “x” is a hexi-decimal digit, 0-f

Layer 2 - Ethernet

- The ethernet address space is flat
- Addressing is not scalable
- Ethernet transmissions are “unreliable”, the receiver does not acknowledge receipt

Layer 3

- Three common layer 3 TCP/IP protocols are
  - IP the inter-networking protocol
  - ICMP the IP control message protocol
  - ARP the address resolution protocol

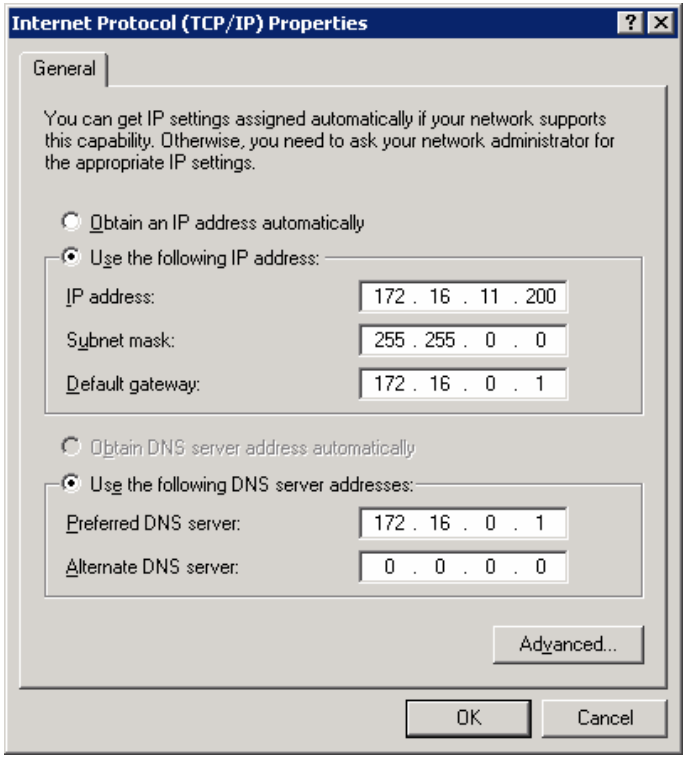
Layer 3 - IP

- Data is packaged in packets
- Contents of an IP packet are
  - source address (4 bytes)
  - destination address (4 bytes)
  - payload
- IP addresses are hierarchical
- Written as
  - ddd.ddd.ddd.ddd
  - where ddd ranges from 0-255

Fundamentals of Computer Networking

Layer 3 - IP

- An IP address consists of a network part and a host part
- Displayed as address and subnet mask
- Can also be displayed as 172.16.11.200/16
- IPv4 addresses are 64 bits
- IPv6 addresses are 128 bits



Layer 3 - ICMP

- These messages convey information about an IP connection
  - Host unreachable
  - Route not found
- This is also the carrier for the ping command
  - ping www.ae.gatech.edu

Layer 3 - ARP

- Address resolution protocol
- Fits between layers 2 and 3
- Creates and maintains the mappings between ethernet addresses and IP addreses

Layer 4 - UDP

- User Datagram Protocol
- Connectionless, send and forget
- Packet ordering not guaranteed
- Does not provide a reliable connection between nodes
- Less expensive to setup than TCP
- Uses source and destination ports for addressing
- Requires IP addressing to locate remote computer

Layer 4 - TCP

- Transmission Control Protocol
- Connection oriented, creates a virtual connection between computers
- Packet ordering is guaranteed
- Does provide a reliable connection between computers
    - will retransmit as necessary
- Uses source and destination ports for addressing
- Requires IP addressing to locate remote computer

Layer 5 - Application

- There are many application level protocols
  - http, smtp, pop, telnet, ssh, smb, nfs, …
- These all rely on the capabilities of the lower levels
- Most are TCP but some are UDP

Packaging Data

- Each layer will add additional content to the data to be transmitted
- For example, an HTTP request will consist of,
  - An HTTP request enclosed in a TCP packet, which in turn is enclosed in an IP packet, which is finally enclosed in an ethernet frame
  - Each level add its own functionality and addressing scheme

Example

- http://www.ae.gatech.edu/

- HTTP request (5) – GET / HTTP/1.0
- TCP packet (4) – specifies port 80
- IP packet (3) – specifies address of web server (128.61.191.2)
- Ethernet frame (2) – puts request on the wire to server (00:50:da:b9:4b:c5)

IP Addresses

- To uniquely identify a connection requires
  - source IP address (3)
  - source port number (4)
  - destination IP address (3)
  - source port number (4)
- Sometimes written as 128.61.191.2:80

IP Addresses - Ports

- The addressing scheme of TCP and UDP uses a source and destination port number
- Both TCP and UDP are point to point in nature – they see only the other computer – they identify a resource on the other end
- Port numbers are assigned and well-known
    - 22 ssh
    - 25 smtp
    - 80 http
    - 3389 rdp
- Source port is usually randomly selected

IP Addresses - Names

- The Domain Name System (DNS), a layer 5 protocol, provides a mapping service between names and addresses
- A name consists of *name.domain*
- The naming system is hierarchical
- Examples
  - www.gatech.edu - 130.207.165.120
  - www.ae.gatech.edu - 128.61.191.2
  - asdlserver.asdl.ae.gatech.edu - 172.16.0.100

IP Addresses – Obtaining

- A computer will usually acquire its IP address from
  - manual configuration
  - from a DHCP (dynamic host configuration protocol) server (a UDP layer 5 protocol)

IP Addresses - Routing

- IP addresses are partitioned into network and host parts
- Computers in the same network are usually on the same ethernet LAN – they do not require routing, they use ARP
- Computers on different networks require a router to reach each other
- Ethernet frames are not routed, only IP packets
- IP configuration will specify a default router address

IP Addresses – Reserved

- The internal loopback address – traffic that stays in the host
  - 127.0.0.0/8
- The private addresses – not routed to the Internet
  - 10.0.0.0/8
  - 172.16.0.0/16 – 172.31.0.0/16 (172.16.0.0/12)
  - 192.168.0.0/24 – 192.168.255.0/24 (192.168.0.0/16)
  - 169.254.0.0/16 - randomly assigned by host

IP Addresses – Reserved

- The non-routed Link Local addresses
  - 169.254.0.0/16
  - 169.254.1.0/24 – 169.254.254.0/24
- A computer that has been configured to acquire its IP address from a DHCP server will select an address from this range after a suitable time-out period has expired

Terms – protocol

- frame – the sequence of bytes in an ethernet transmission
- packet – the sequence of bytes in IP based protocols
- TCP/IP – the DoD created protocol suite used for the Internet
- ethernet – the Xerox created protocol used for LAN's
- tcp stack – refers to the software implementation of the network model
- DNS name – the name associated with an IP address
- IP address – the address of a host using TCP/IP
- MAC address – the address used by ethernet frames

Terms – network devices

• firewall – a device that filters packets based on content or addresses, usually also an IP router

• router – a device that connects IP network segments

• bridge – a device that connects ethernet segments

• proxy – a device that connects to a network service on your behalf

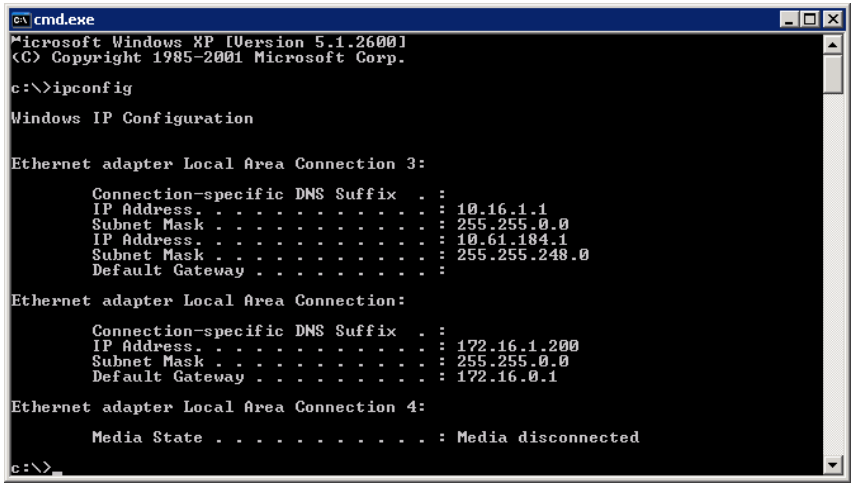
• vpn – virtual private network, a device that creates a virtual network on a public network (Internet). It is usually encrypted.

Windows Network Commands

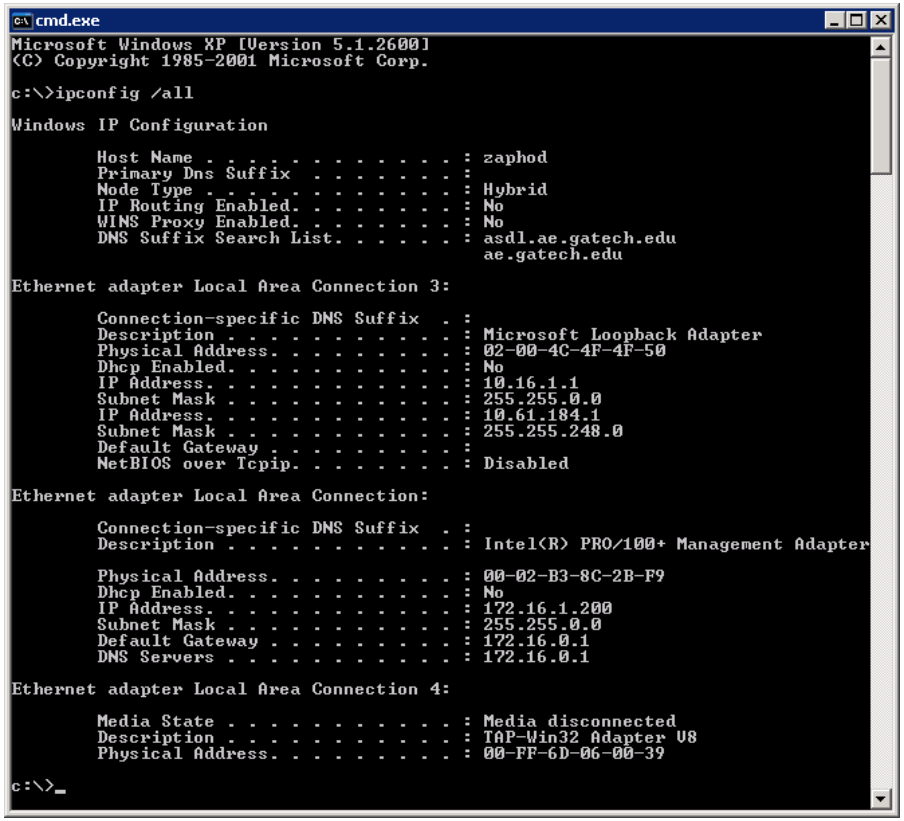
- ipconfig – a command that will display configuration of all network devices (see ipconfig /help)
  - ipconfig /all
  - ipconfig /release and ipconfig /renew
- route – a command that will configure and display the current route tables on your computer (see route help)
  - route – route add 192.168.10.0 mask 255.255.255.0 192.168.10.50
  - route print
- netstat – a command to display current network connections (see netstat help)
  - netstat – default to display current TCP connections
  - netstat –a – display all connections, including listening
- tracert – this command will display the path to the target host
  - tracert www.ae.gatech.edu
- ping – send a ping packet to the remote host (some hosts do not respond)
  - ping www.ae.gatech.edu
- nbtstat – display MS specific network info (see nbtstat help)
  - nbtstat –A asdlserver.asdl.ae.gatech.edu

Fundamentals of Computer Networking

Windows - ipconfig

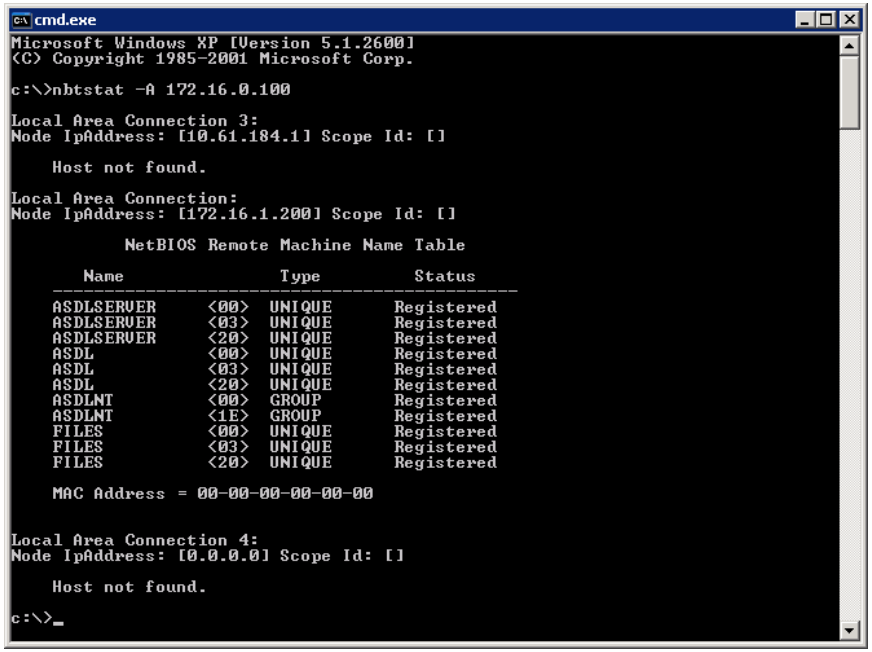


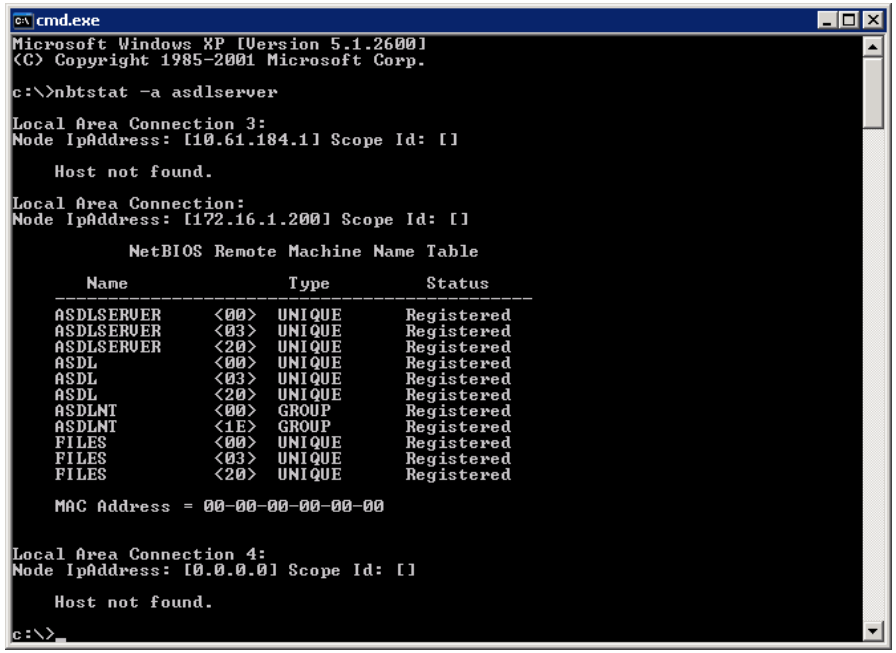
The ipconfig command will display the current IP configuration of a windows computer.



Fundamentals of Computer Networking

Windows - nbtstat

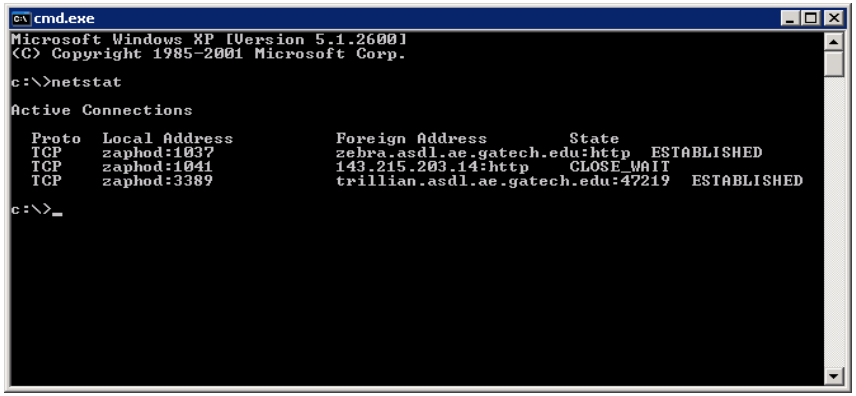


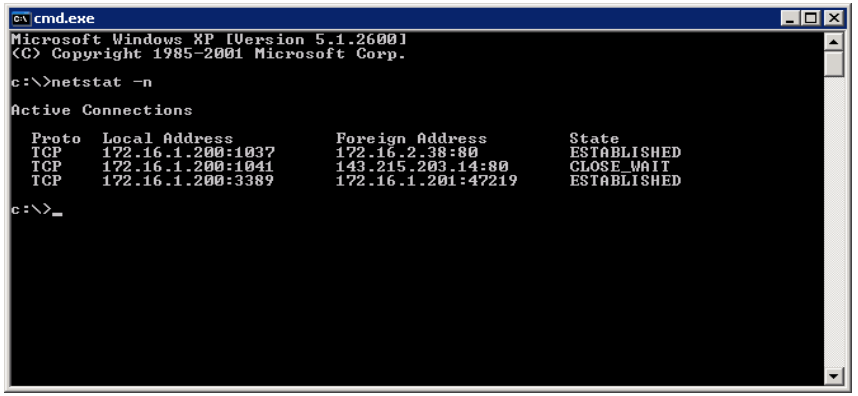


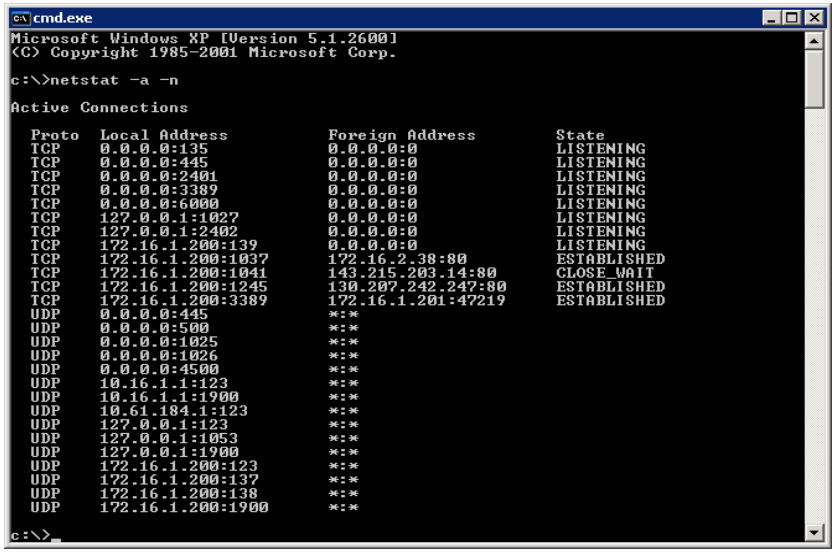
The nbtstat command displays information about other Windows systems on the network. It accepts either DNS name or NetBIOS name.

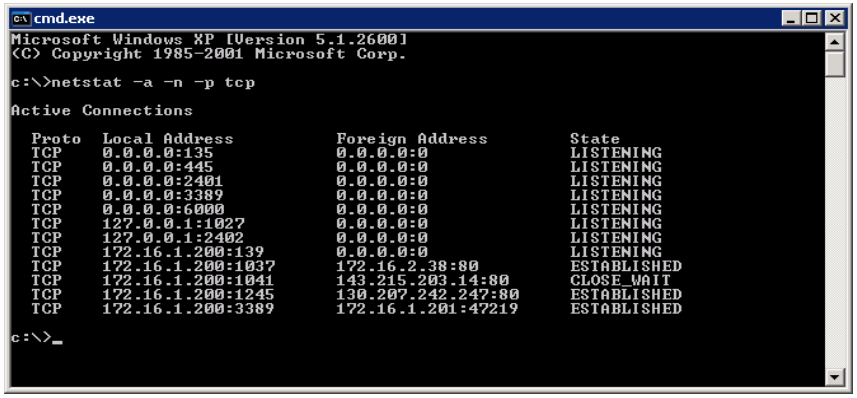
Fundamentals of Computer Networking

Windows - netstat



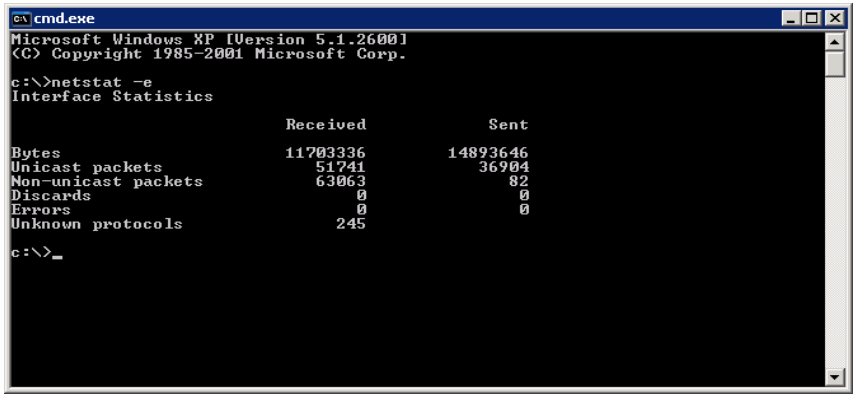


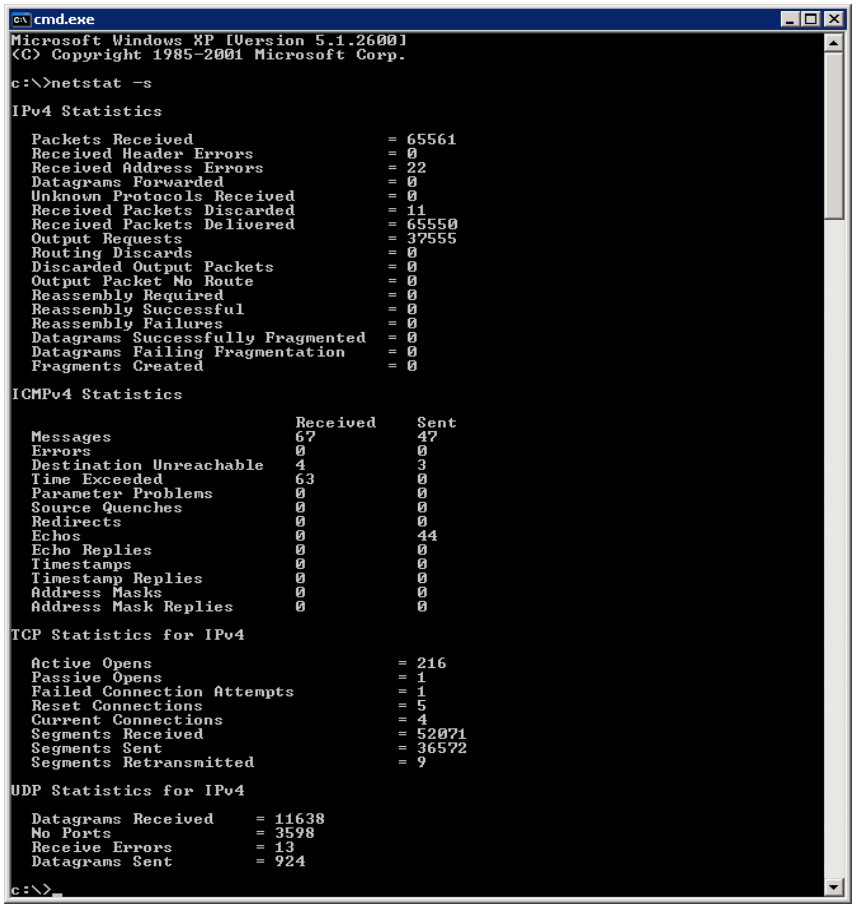




Fundamentals of Computer Networking

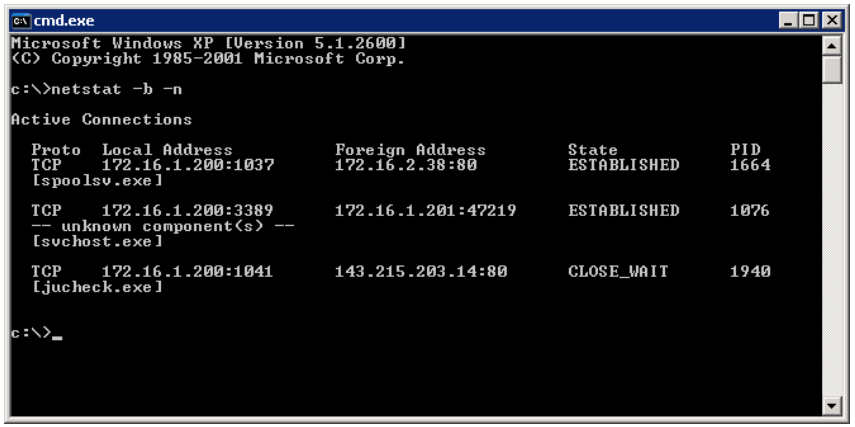
Windows - netstat

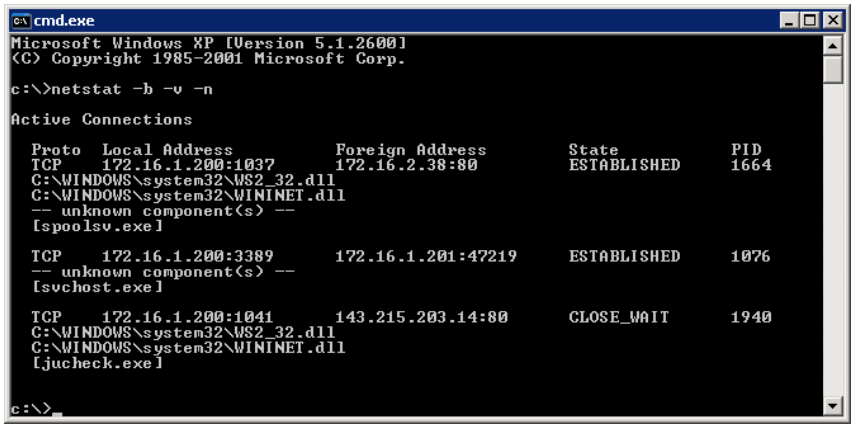


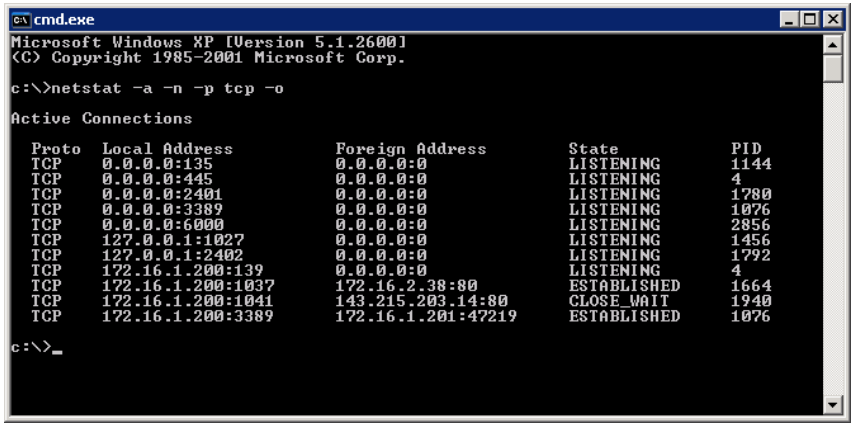


Fundamentals of Computer Networking

Windows - netstat

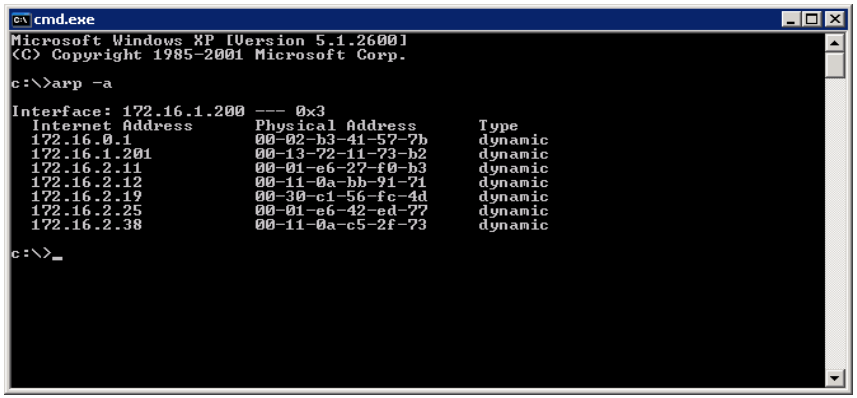


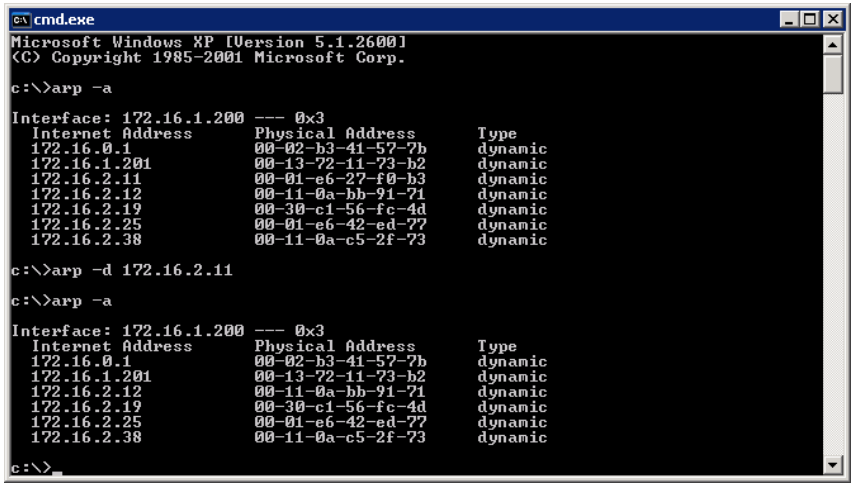




Fundamentals of Computer Networking

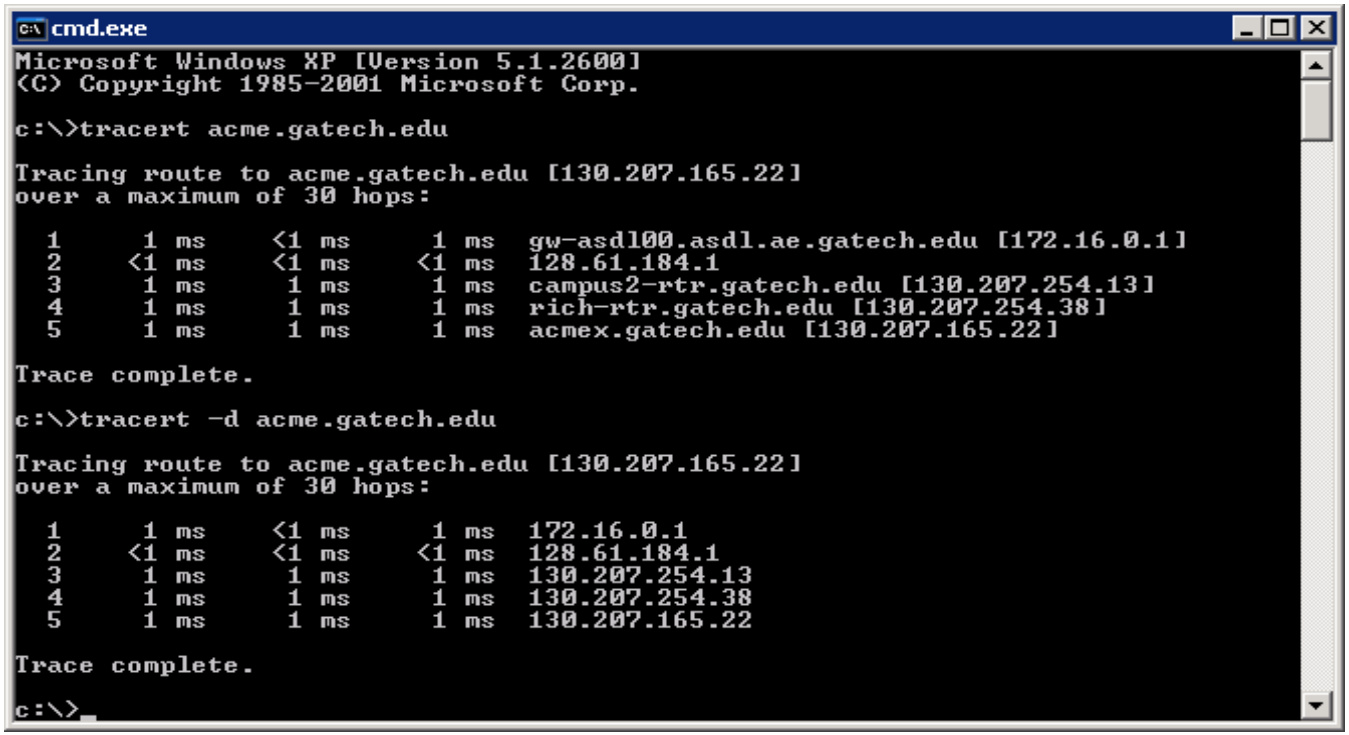
Windows - arp





Fundamentals of Computer Networking

Windows - tracert



Linux/Unix network commands

- ifconfig – configure and display network devices
  - ifconfig eth0 – display configuration of eth0
- route – configure and display the hosts route tables
  - route – display route table
- ip – multi-purpose network command
  - ip addr – display network configurations
  - ip route – display route table
- netstat – display current network connections
  - netstat – display all current tcp and udp connections
  - netstat –at – display all current tcp connections including listening ports

Linux/Unix network commands

- traceroute – display the path to remote host
    - traceroute www.ae.gatech.edu
- ping – send a ping to the remote host
    - ping www.ae.gatech.edu