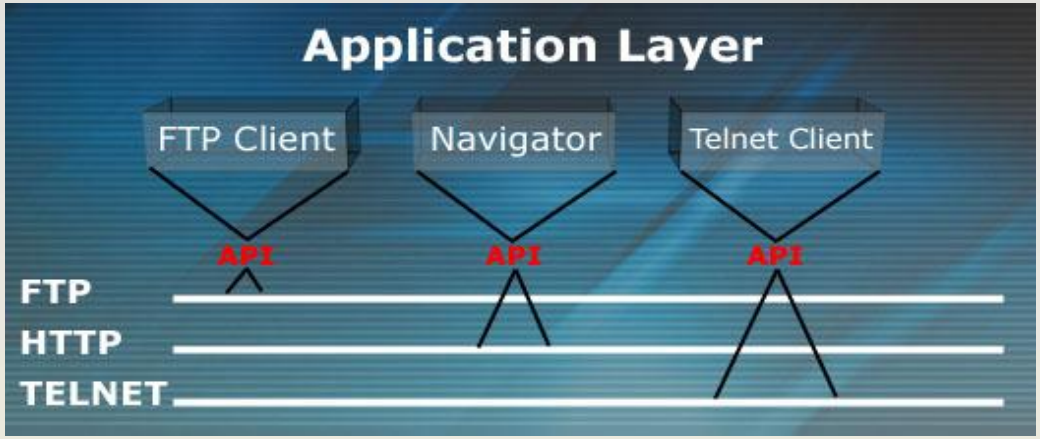
PROTOCOLS

Protocols Overview

OSI MODEL	TCP/IP	ICMP
UDP	ARP	DNS
SSH	SNMP	SMTP

OSI – Application Layer



Functionality

- Protocols at this layer allow the applications to communicate to applications on remote systems
- This is not where applications work, but the protocols that support the application's networking functionality
- Some of the protocols at this layer
  - SMTP, HTTP, LPD, FTP, Telnet, and TFTP

OSI – Presentation Layer

Functionality

- No protocols work at this layer, only services
- Only concerned with syntax of data
  - Data conversion into standardized format
  - GIF, ASCII, Unicode, JPEG, TIFF
- Other functionality that take place at this layer
  - Encryption, decryption, compression, decompression

OSI – Session Layer

Functionality

Dialog management between programs

- Access control, recovery, synchronization

Setup, maintenance, session tear-down of session communication channels

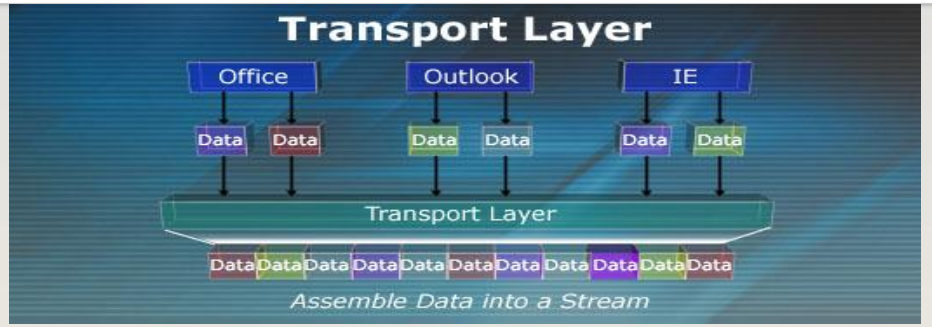
Depending on the protocol at this layer, communication can take place…

- Full-duplex = two-way conversation at the same time
- Half-duplex = only one application can communicate at a time

Some protocols that work at this layer:

- SQL, NFS, RPC

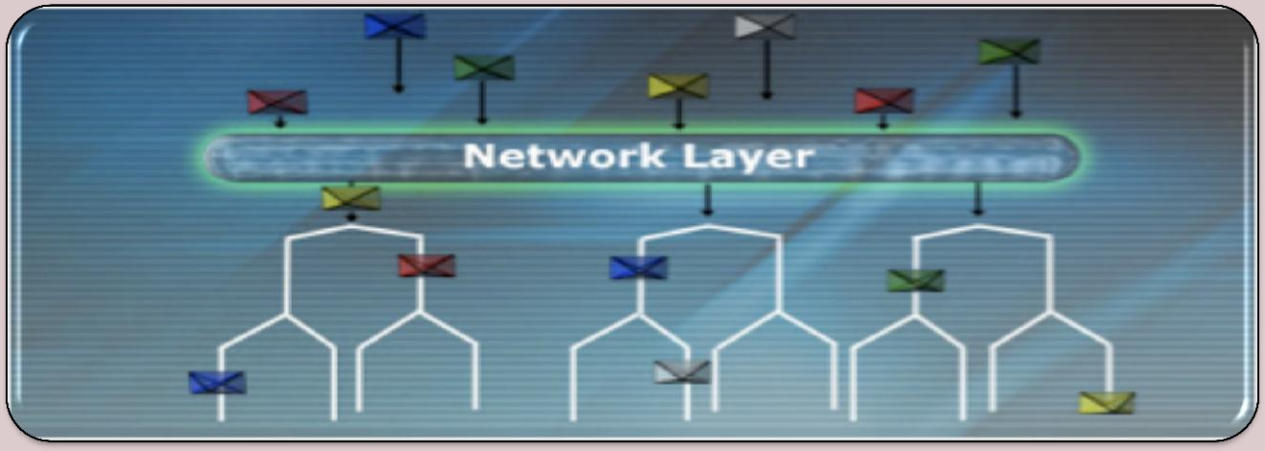
Transport Layer



Functionality

- End-to-end packet transfer using connection-oriented or connectionless protocols
- Transport protocols are concerned with getting data from one system to another
  - Does not work with application-to-application communication
- Use of ports to communicate with higher-level protocols and to track different communications taking place
- Segmenting appropriate size of packets for processing by the network layer
- Some protocols that work at this layer:
  - UDP, TCP, SPX

OSI – Network Layer



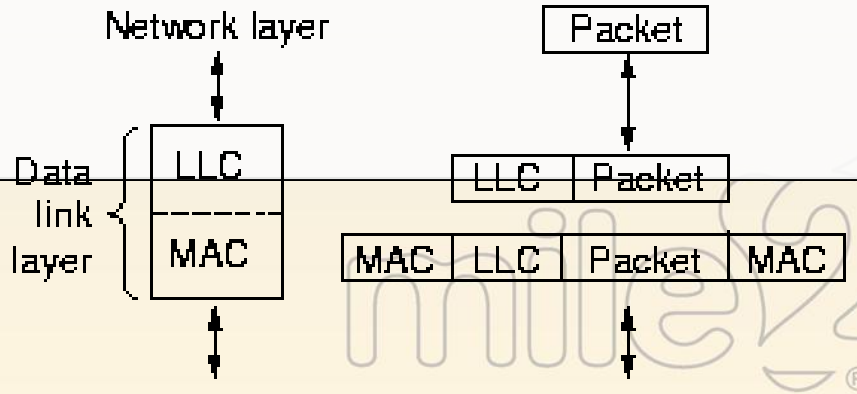
Functionality

- Routing of packets and addressing takes place here
  - Routing protocols work at this layer
  - When a packet is sent down from the transport layer, the network layer protocol adds the address and creates a network header
- Confidentiality, authentication and integrity can be provided at this layer
  - Through IPSec
- Some protocols that work at this layer:
  - IP, RIP, ICMP, IGMP, IGRP, BGP

OSI – Data Link

Data Link Functionality

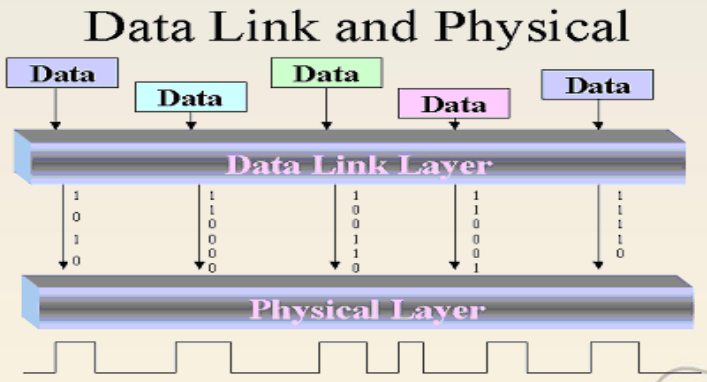
- Sender breaks data into frames and transmits sequentially
- Formats frame for proper technology (Token Ring, Ethernet, ATM)
  - Referred to as framing
- Media access (token passing, CSMA, polling) takes place at this layer
- Synchronization and error control
- Has two sub layers
  - 802.2 – Logical Link Control (LLC) layer
  - 802.3 – Media Access Control (MAC) layer – Ethernet
    - 802.11 – WLAN
    - 802.5 – Token Ring



OSI – Physical Layer

Physical Functionality

- Bits turned into voltage
  - Encoding of voltage binary representation varies between different LAN, MAN, and WAN technologies
- Provides standards for interfaces to media
- Type of electrical signaling and format depends upon transmission type
  - Photons for fiber
  - Electrical voltage for Ethernet
- Radio frequencies for wireless

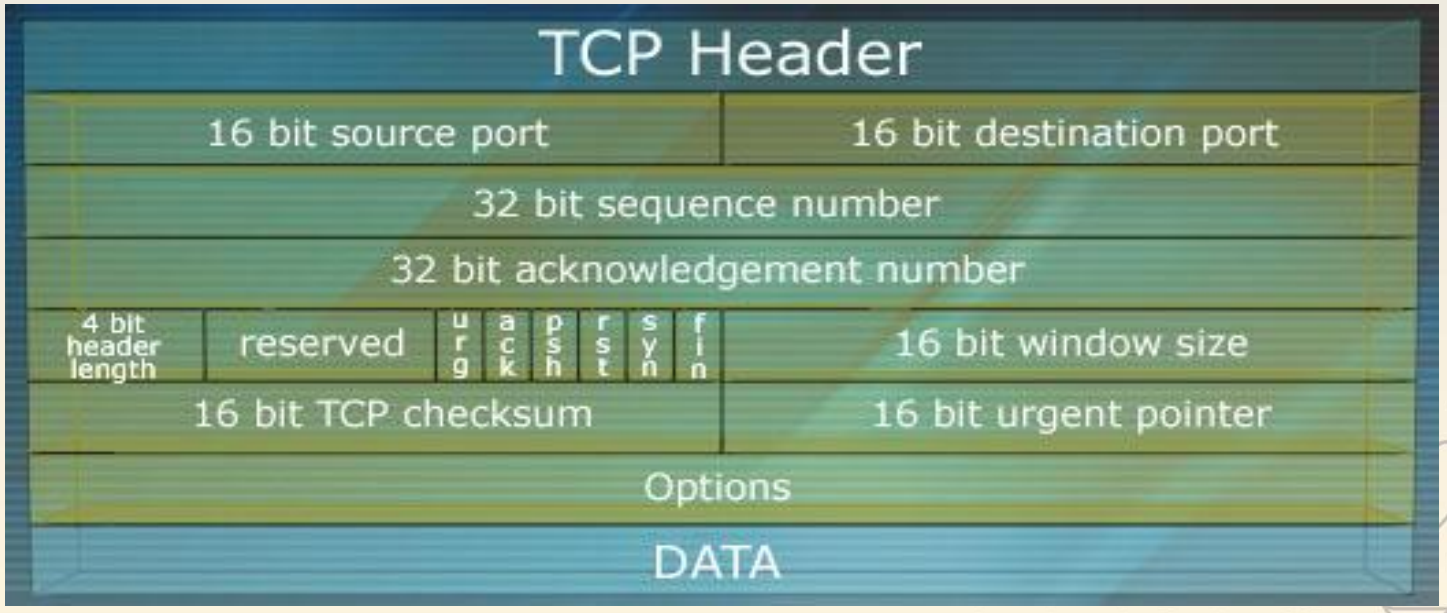


Protocols at Each OSI Model Layer

OSI LAYER	PROTOCOLS
Application	DNS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; TELNET; HTTP
Presentation	ASCII; TIFF; GIF; JPEG; MPEG; MIDI; MIME
Session	NetBIOS; NFS; SQL; RPC
Transport	TCP; UDP; SPX; SSL
Network	IP; ICMP; RIP; IGMP; IPX
Data Link	SLIP; PPP; ARP; RARP; L2F; L2TP
Physical	High-speed Serial Interface(HSSI); X.21; EIA/TIA-232 and EIA/TIA-449

Protocols of the Internet

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- TCP = connection-oriented transport layer protocol
- IP = connectionless network layer protocol
- Suite of protocols that govern how data travels over a network



Port and Protocol Relationship

TCP/IP Suite Usage of Ports

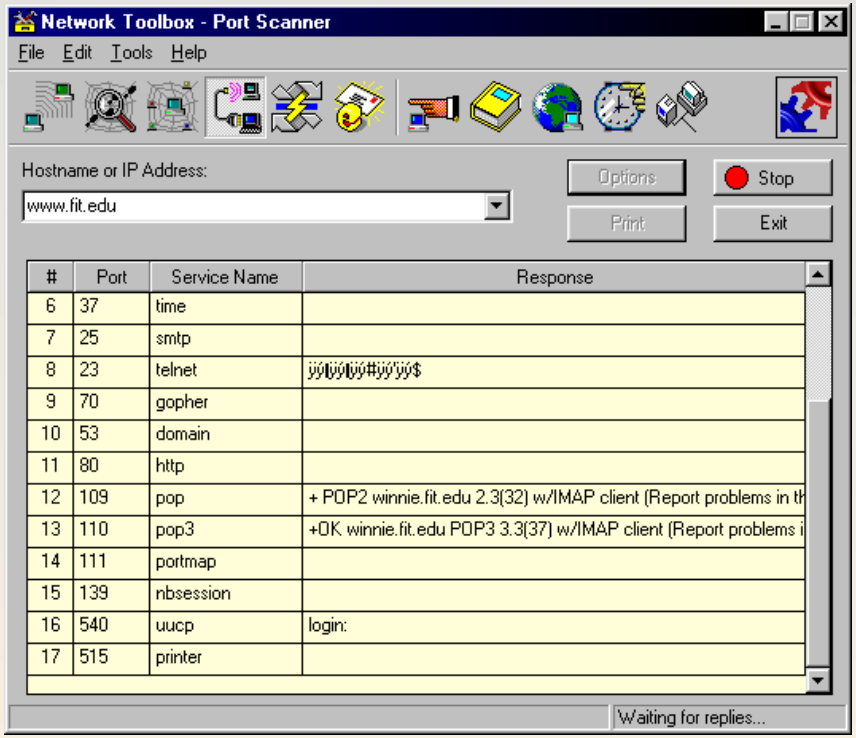
Port numbers mapped to specific protocols

Well-known ports are 0-1023

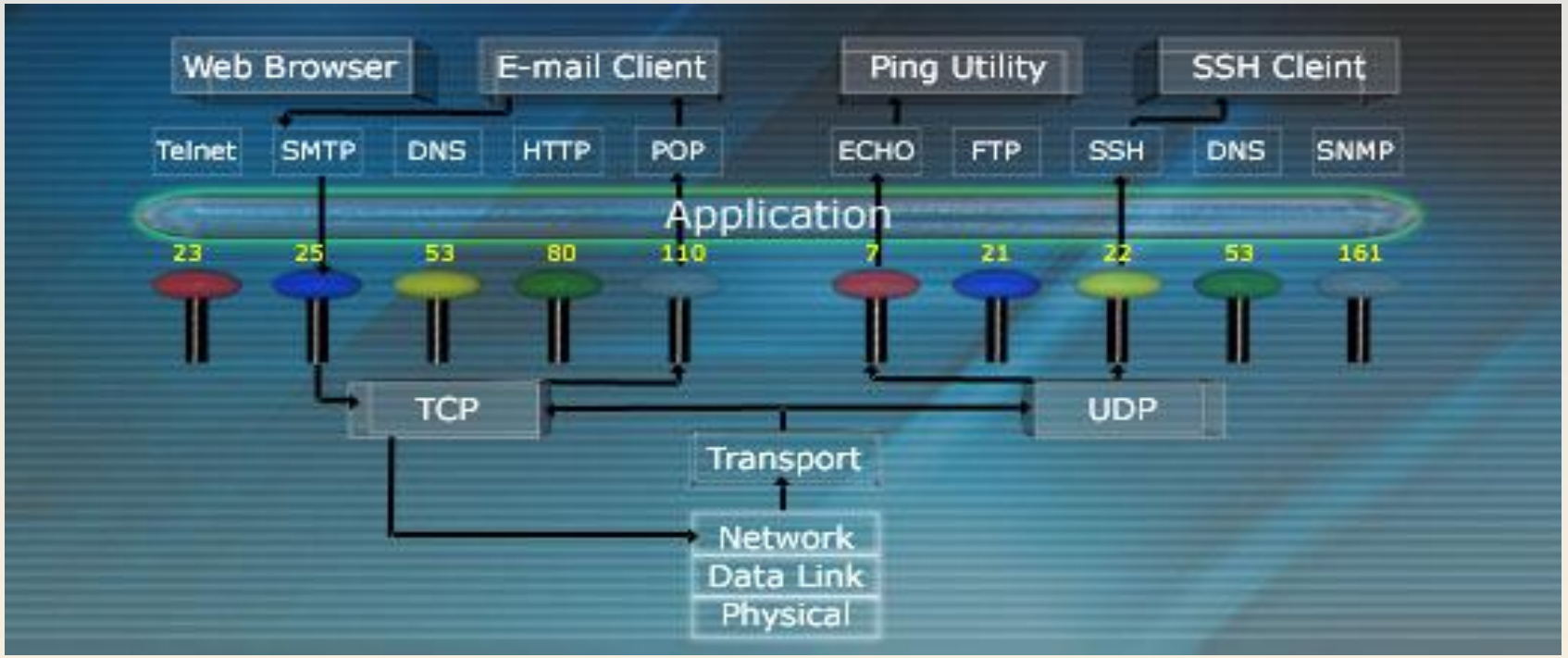
- FTP port 20 and 21
- SMTP port 25
- SNMP port 161
- HTTP port 80
- Telnet port 23

Source port is usually a high dynamic number, while the destination port is usually under 1024

TCP and UDP uses ports to communicate with upper layer protocols



Conceptual Use of Ports



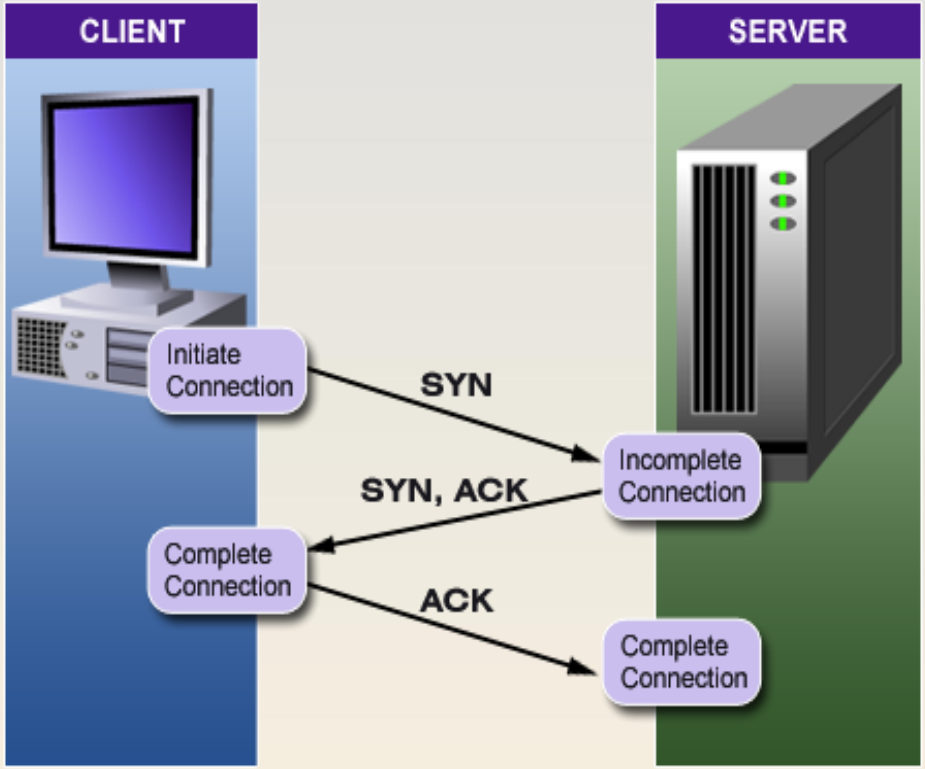
UDP versus TCP

TCP

- Connection-oriented
- Reliable
- Performs a setup handshake
- Error detection and correction
- Windowing

UDP

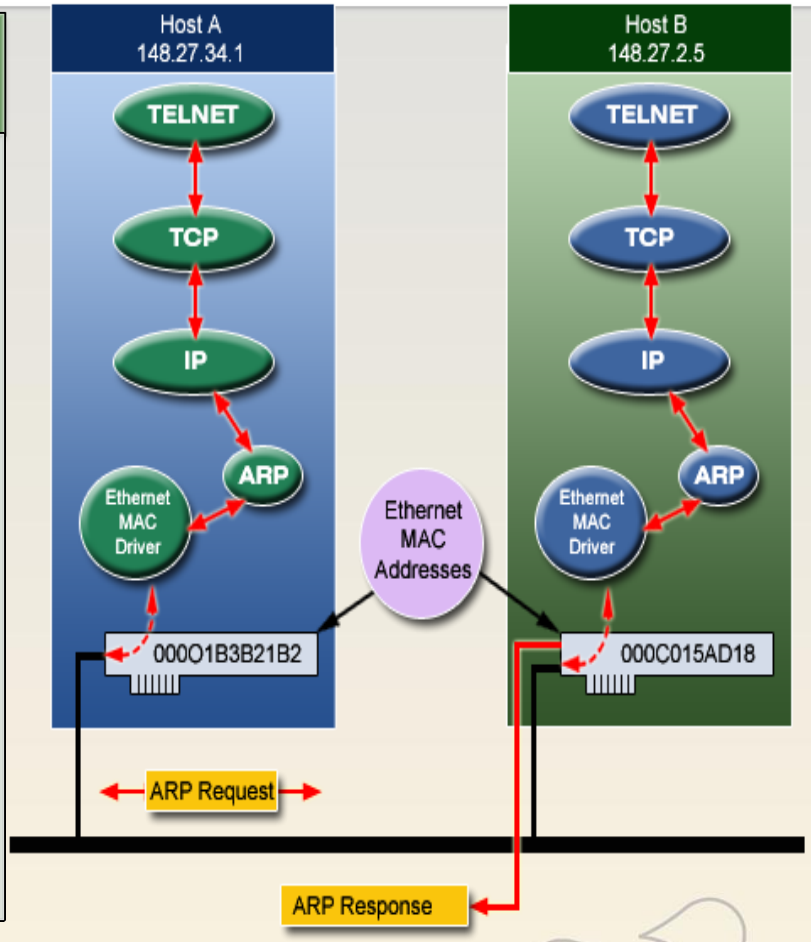
- Connectionless
- Unreliable
- No handshake is performed
- “Best effort” protocol



Protocols – ARP

Address Resolution Protocol

- Maps the IP address to the media access control (MAC) address
  - IP address = 32-bit software assigned
    - Network layer
  - MAC address = 48-bit hard-wired into NIC
- Data link Layer
- Data link layer protocols understand MAC addresses, not IP addresses



Protocols – ICMP

Internet Control Message Protocol

Status and error messaging protocol

- Not used to move user data

Ping utility uses this protocol

- ICMP ECHO request and reply

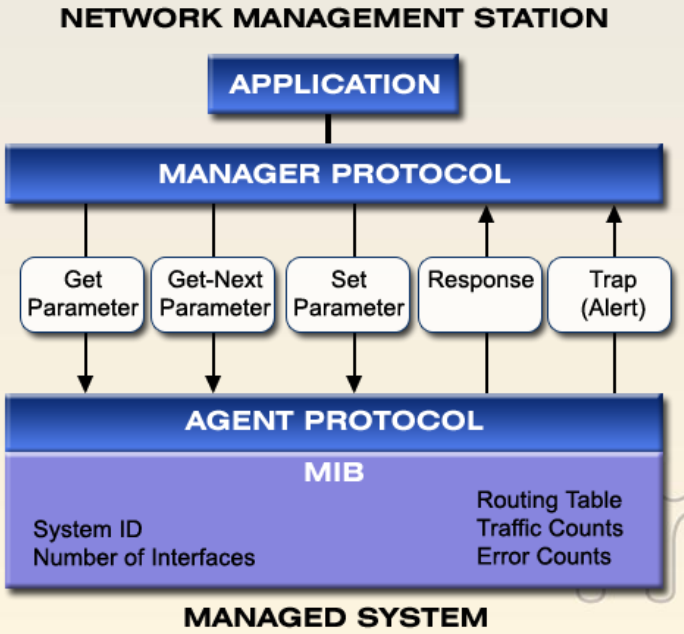
ICMP Uses by Hackers

Allowed through most firewalls

- Used for host enumeration

Redirect traffic by sending bogus ICMP messages to router

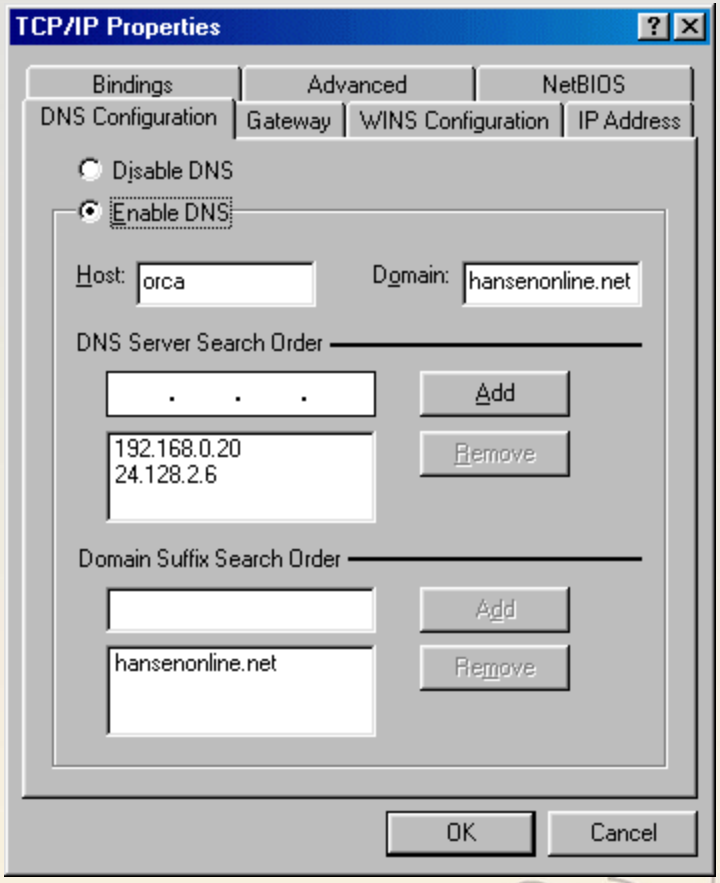
- Router thinks that another router is telling it that a link is down or congested



Network Service – DNS

- **Works within a hierarchical naming structure**
- **Hostname to IP address mapping**
- **DNS server that holds resource records for a zone is the authoritative DNS server for that zone**

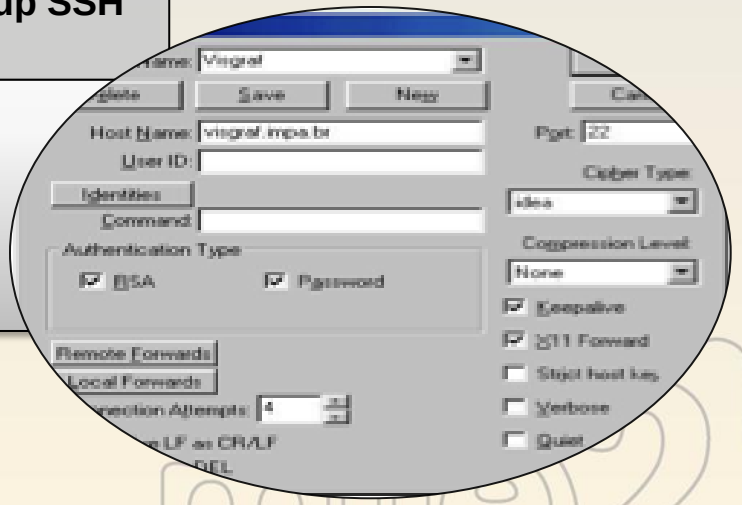
Domain Name Service



SSH Security Protocol

- Secure access to remote systems
  - Can run different protocols and applications through a SSH tunnel
- Should be used instead of Telnet and r-utilities
- Server and client generate their own private/public key pairs
- Many times uses Diffie-Hellman for its key agreement protocol
- Like many other protocols, must carry out a handshake process
  - Agree upon parameters to set up SSH tunnel

Secure Shell (SSH)



SSH

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

- Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for TELNET and other insecure remote shells, which send information, notably passwords, in plaintext, leaving them open for interception.
- The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.[1]

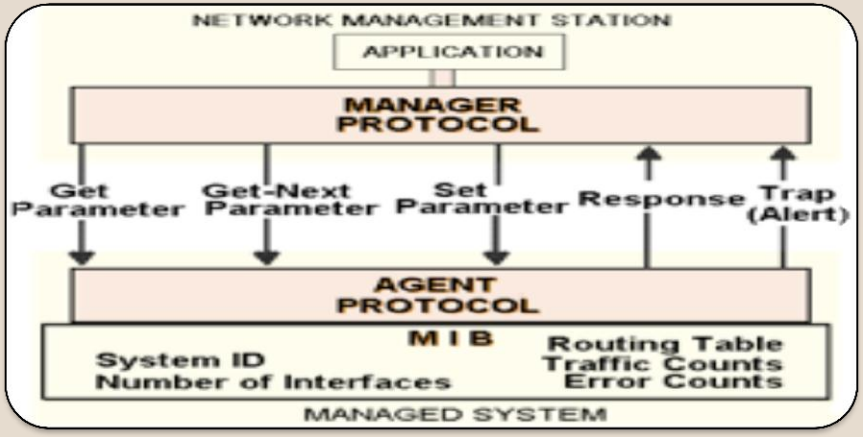
SSH is typically used to log into a remote machine and execute commands but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols.[1] SSH uses the client-server model.

An SSH server, by default, listens on the standard TCP port 22.[3]

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, FreeBSD, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist.

http://en.wikipedia.org/wiki/Ssh

Protocols – SNMP

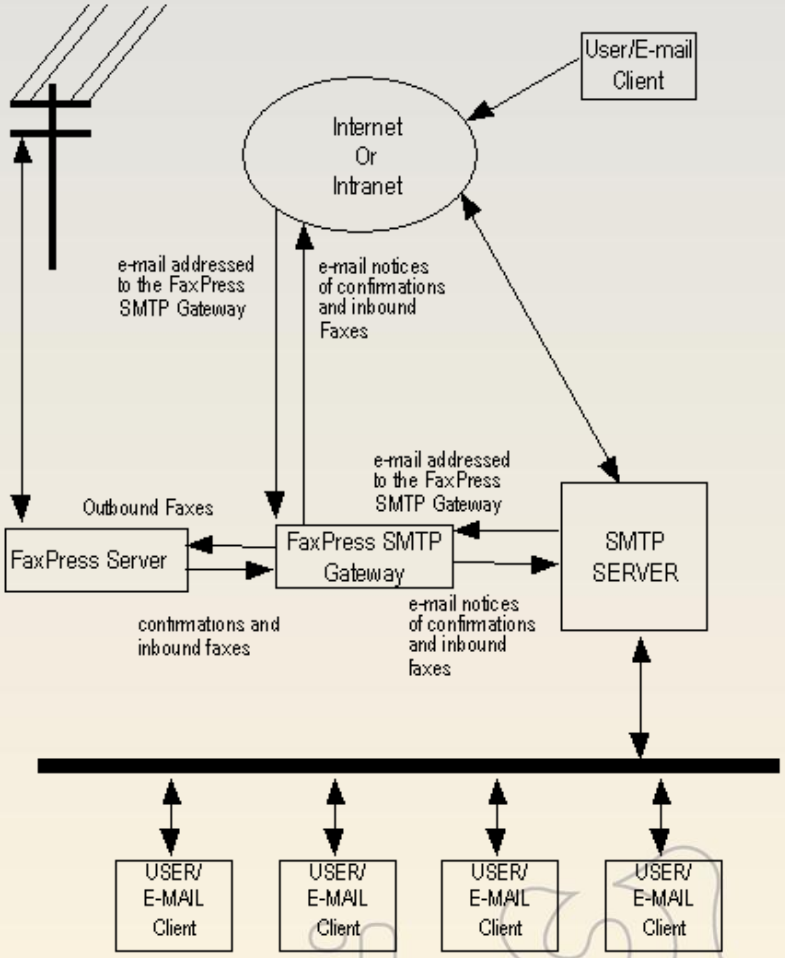


Simple Network Management Protocol

- Master and agent model
- Agents gather status information about network device
- Master polls agent and provides an overall view of network status
- Community strings = public and private
  - Public = Read MIB data
  - Private = Read/Modify MIB data

Simple Mail Transfer Protocol

- Transmits mail between different mail servers
- Protocol to send outgoing mail from e-mail clients
- Security issue with mail servers = improperly configured mail relay
  - Servers identified and used by spammers
  - Companies get blacklisted by other companies without knowing why



Review

OSI MODEL	TCP/IP	ICMP
UDP	ARP	DNS
SSH	SNMP	SMTP