NSCOM01

UDP-Based Application Protocols

3rd Term– AY2022 – 2023

Instructor: Dr. Marnel Peradilla

USER DATAGRAM PROTOCOL

- **The User Datagram Protocol (UDP) is a connectionless transport protocol used in TCP/IP networks**
- **Considered as a 'bare-bones' protocol that provides only the essential capabilities needed to transport a data segment between applications**
- **Features:**
  1. Unreliable – datagrams are not acknowledged
  2. No congestion control mechanism- datagrams sent as quickly as possible
  3. Stateless – Server does not keep track of status and session information of a client. Each request-response exchange with a client is treated as an independent transaction
  4. Unordered delivery – datagrams do not contain any sequencing information

WHEN TO USE UDP

- **Connectionless services are commonly used with applications where occasional data loss is tolerable in exchange for reduced protocol overhead:**
  1. Inward Data Collection – periodic sampling of data sources such as sensors or automatic self-test reports from network equipment
  2. Outward Data Dissemination – message broadcasting to nodes or distribution of data to a network
  3. Request – Response – query-based applications that use a transaction service provided by a single server where a single request-response is typical
  4. Real-time applications – applications with a degree of redundancy or real-time requirement e.g. voice, telemetry

APPLICATION PROTOCOLS

- **Several well-known application protocols use UDP as transport protocol to support their operations:**
  - System Logging Protocol
  - Network Time Protocol
  - Domain Name System
  - Dynamic Host Configuration Protocol
  - Trivial File Transfer Protocol
  - Simple Network Management Protocol

TFTP

Trivial File Transfer Protocol

TFTP

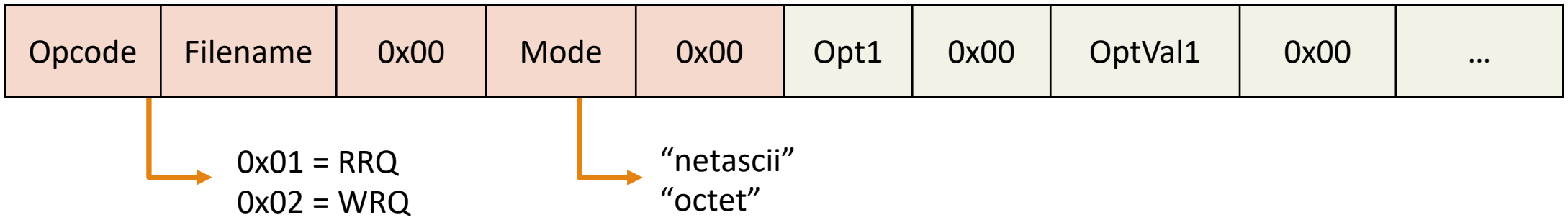
- RFC 783 and 1350 then later extended using several RFCs
- Very simple protocol for downloading or uploading files to and from a server usually within a LAN setting
- Commonly used to boot diskless devices over a network or to copy network appliance (e.g .router, switch) firmware or configuration files to/from a server
- Minimal network overhead and resource requirements due to simplicity of design and its use of UDP as its transport layer protocol

PROTOCOL CHARACTERISTICS

- Uses UDP **port 69** on the server to listen for requests, but switches to another port for replies to free up port 69
- Simple request-acknowledgment protocol - each data packet needs to be acknowledged before the next data packet may be sent (lock-step method)
- Uses positive acknowledgement method - only correctly received packets are acknowledged. Retransmission is required if a transmission is not acknowledged within a time limit

TFTP MESSAGES

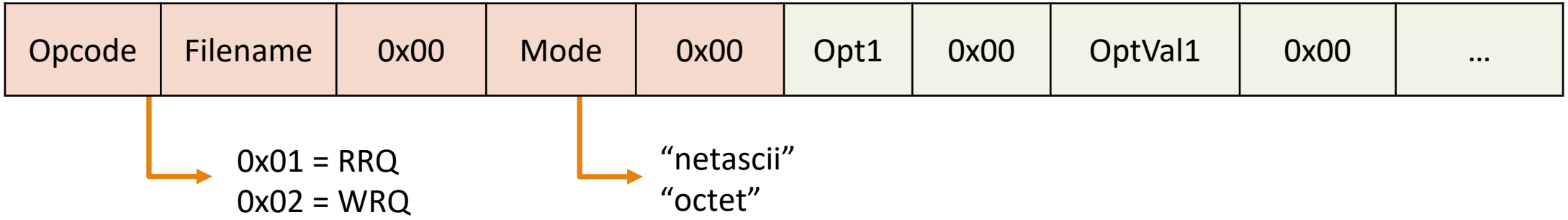
- **Read or Write Request (RRQ or WRQ) is used to signal a file download or upload request to the server**



- **Both filename and transfer mode are variable length strings with the 0 byte serving as null terminator**
- **Transfer Modes:**
  - “netascii” - Used as a standard format for transferring text files.
    - All lines need to end with \r\n (ASCII carriage return + line feed)
    - Both ends responsible for converting to/from netascii format.
  - “octet” - Used for transferring binary files. No translation done.

TFTP MESSAGES

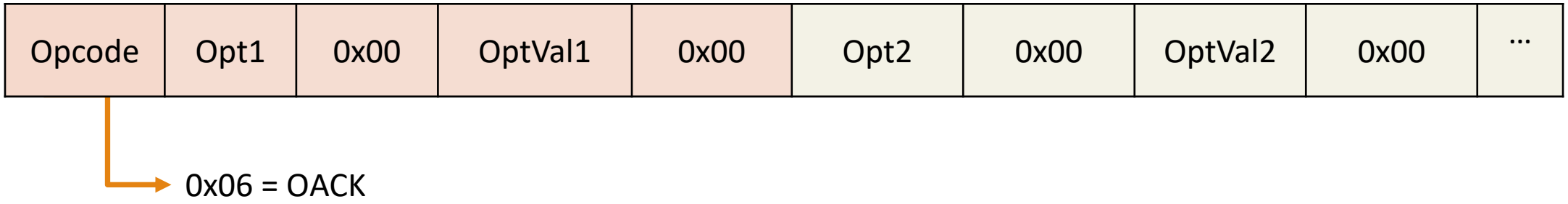
- **Read or Write Request (RRQ or WRQ) is used to signal a file download or upload request to the server**



- **Additional options may be requested by a client by adding Option-Value pairs at the end of an RRQ or WRQ. Values are always sent as an ASCII string**
  - “blksize” – to specify the file transfer block size
  - “timeout” – number of seconds to wait for a reply before retransmit of previous packet
  - “tsize” – used to inform the server of the total size of the file to be uploaded when doing an WRQ

TFTP MESSAGES

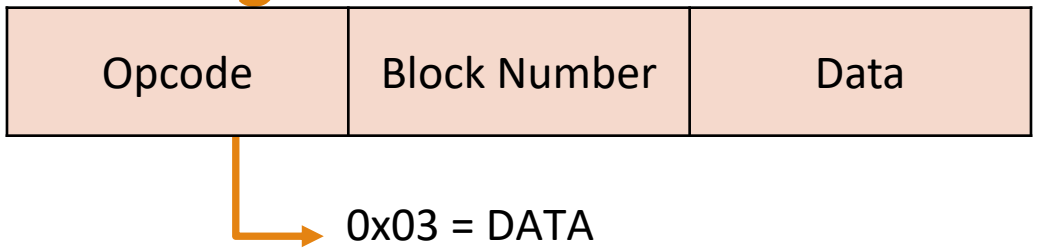
- Option Acknowledge (OACK) messages are used to reply to a read or write request

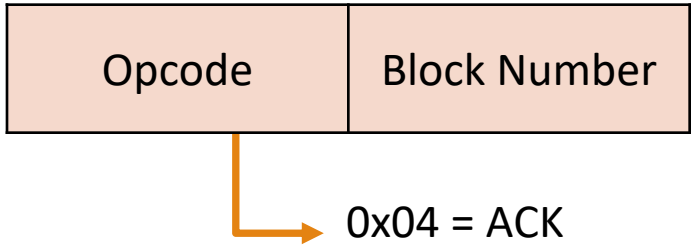


- Options in an OACK will include the only the option names and respective values that were accepted by the server
- If a requested option is not included in the OACK, it means that the option was not accepted by the server

TFTP MESSAGES

- **Data and acknowledgment messages are used to transfer blocks of the file being transferred**

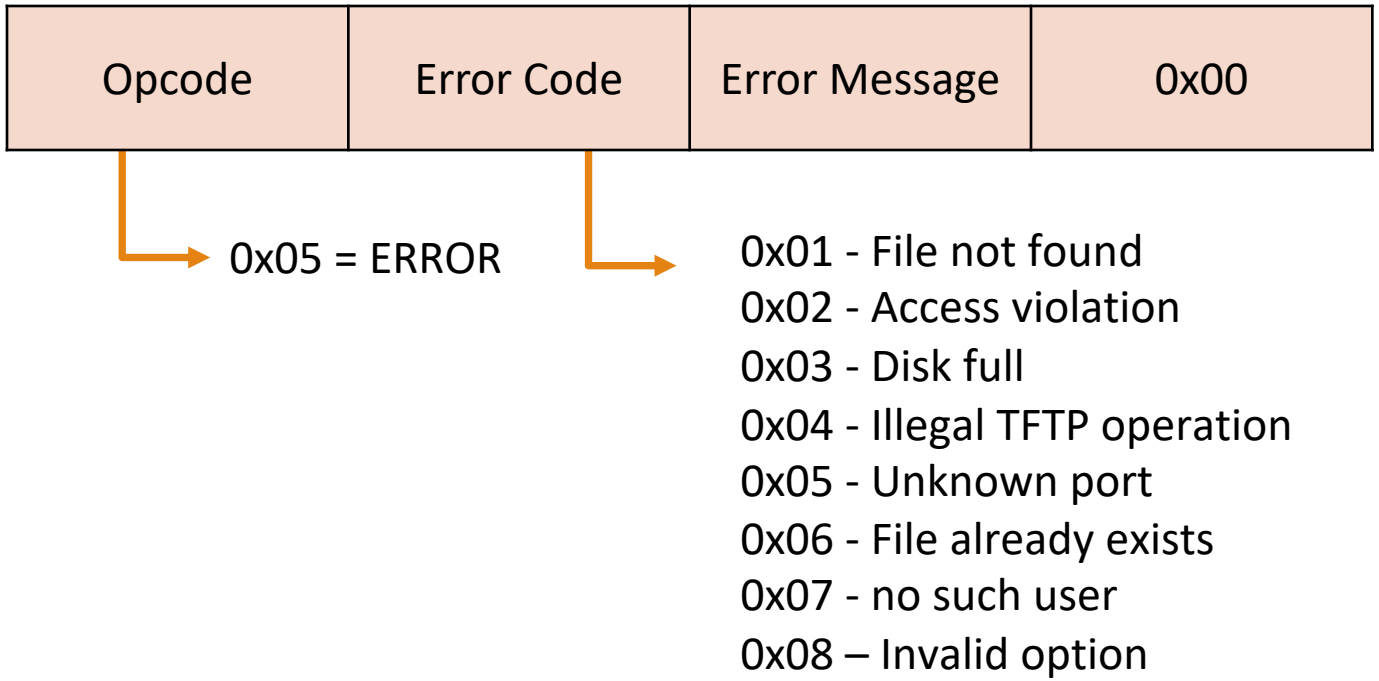




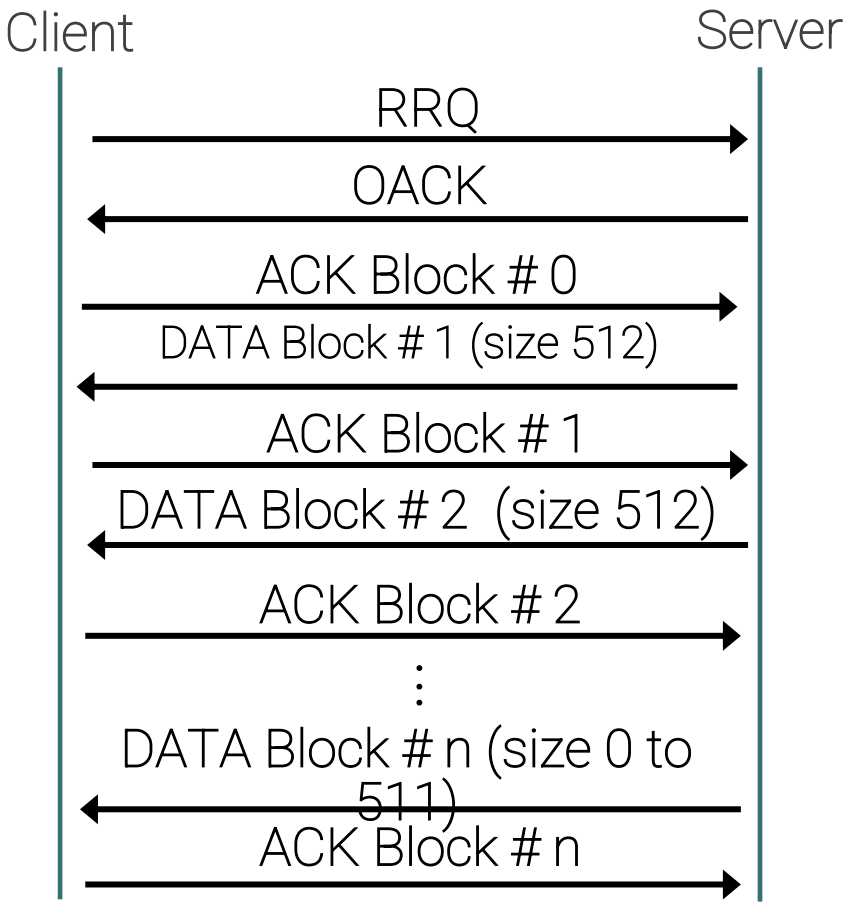
- Block number is used to indicate the sequence number of the data block
  - Used for reassembly at the receiver and to signal back which block was received to the sender
- Data field contains a portion of the file being transferred (by default 512 bytes)
  - A data field with less bytes than the negotiated block size signals the end of the file
  - If last block of the file is the same size as the block size option, another DATA message with 0 bytes data field needs to be sent
- An ACK can be also be sent to acknowledge a WRQ if no negotiated options are accepted
- The sending host can send the next DATA block only if an ACK to the previous block was received

TFTP MESSAGES

- **Error message is used to signal an error condition in response to an RRQ or WRQ**



TFTP READ SEQUENCE



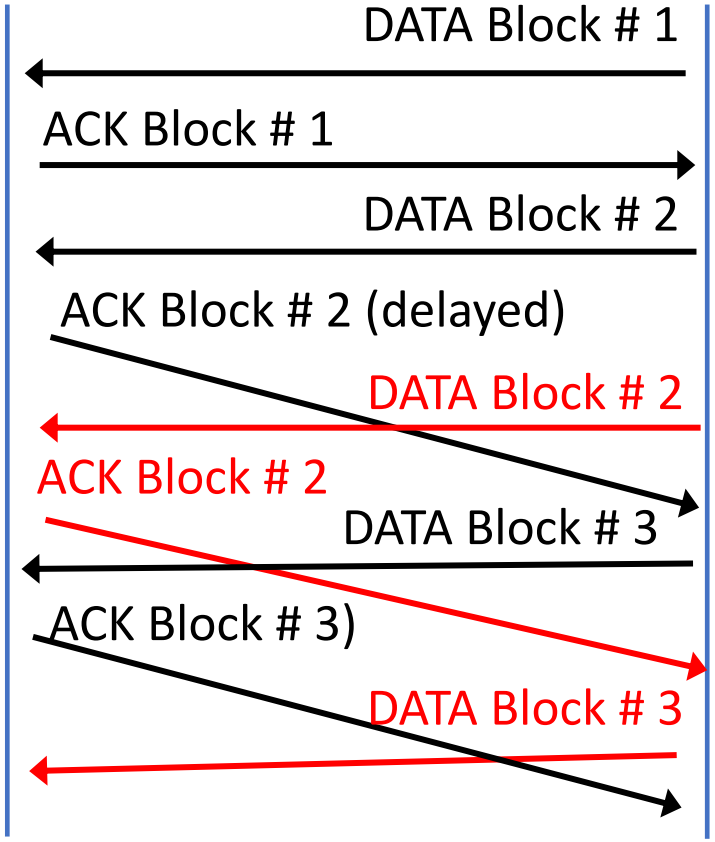
Initiate transfer with a read request packet (RRQ).
The server responds with an OACK to accept options, are immediately to Data Block 1 if options cannot be accepted

First data block is sent from the server and the client acknowledges the reception of the first data block.

The transfer continues with the next data block which is acknowledged by the client.

The last data packet contains 0 – 511 bytes. This signals
the end of transfer to the client.
The transfer is completed by the last acknowledge.

SORCERER'S APPRENTICE PROBLEM



Retransmit 2 due to timeout

2 copies of each packet from here onwards

- **This original protocol suffers from the "sorcerer's apprentice syndrome.**
  - Each message received triggers the sending of a packet
  - Sender uses a timeout for acknowledgment – If data is not acknowledged within a time limit, the last data block will be retransmitted
  - Issue: Delayed ACKs can trigger a cascade of duplicate transmissions
- **Revised protocol requires that duplicate ACKs should be recognized and ignored. only the first instance of a received acknowledgment should cause the next data block to be sent**

TFTP LIMITATIONS

- Lock-step method eliminates the need for flow control but will limit throughput
- Does not provide any authentication and access control mechanism – hence any file may be uploaded or downloaded from the server
- No integrity checking – possible to receive damaged data
- Does not support listing, deleting, or renaming files

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."