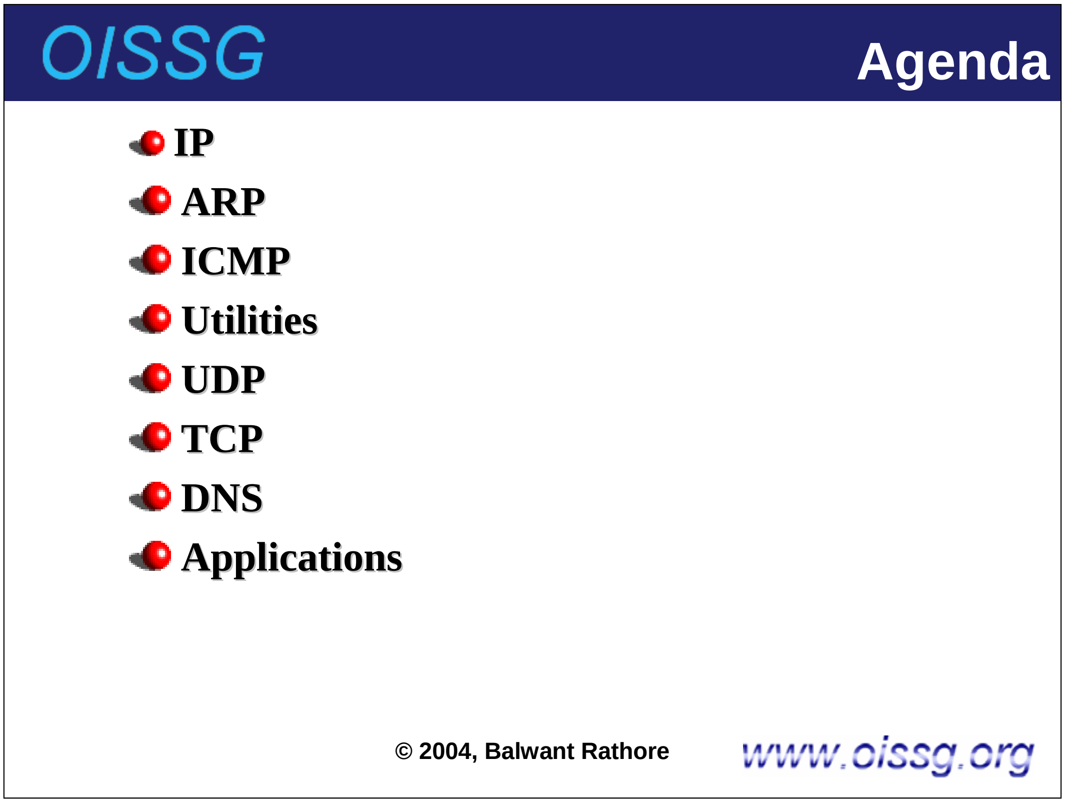
OISSG

FIST Conference 2004, Jaipur
March Edition

Refreshing TCP/IP

Balwant Rathore, CISSP
CEO, Segress Technologies Ltd.,
Vancouver, Canada
Founder Open Information System Security Group
www.oissg.org

www.oissg.org

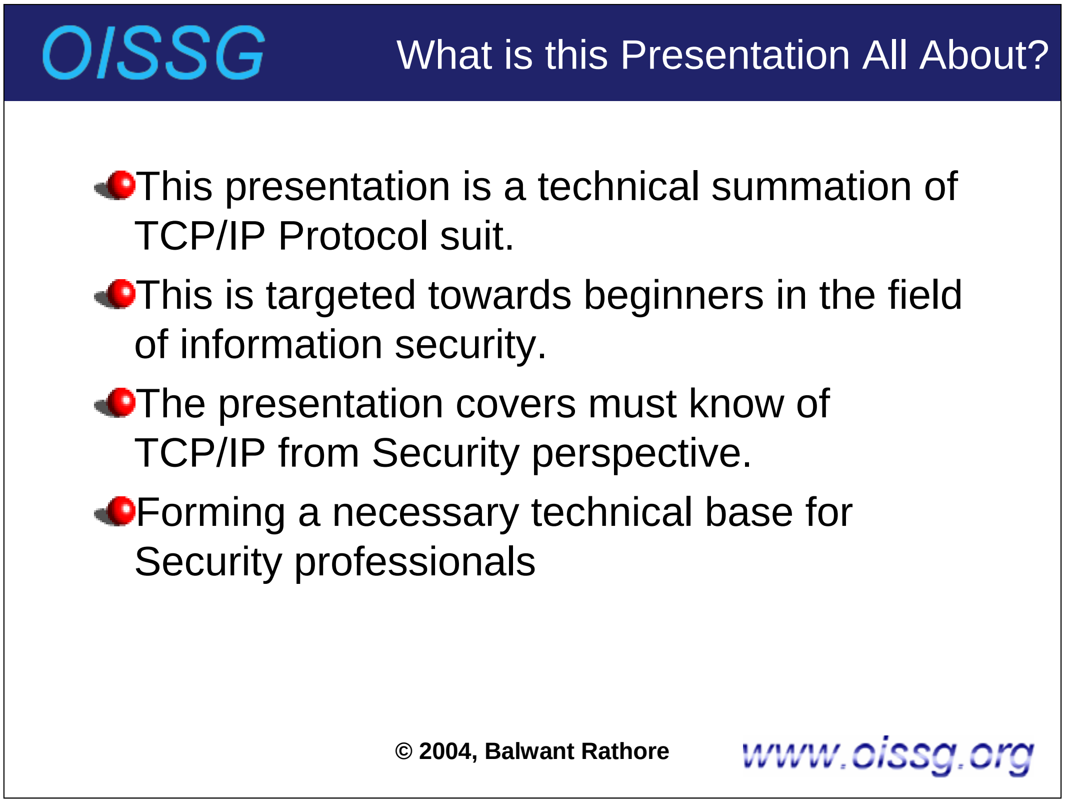


OISSG

Agenda

- IP
- ARP
- ICMP
- Utilities
- UDP
- TCP
- DNS
- Applications

www.oissg.org

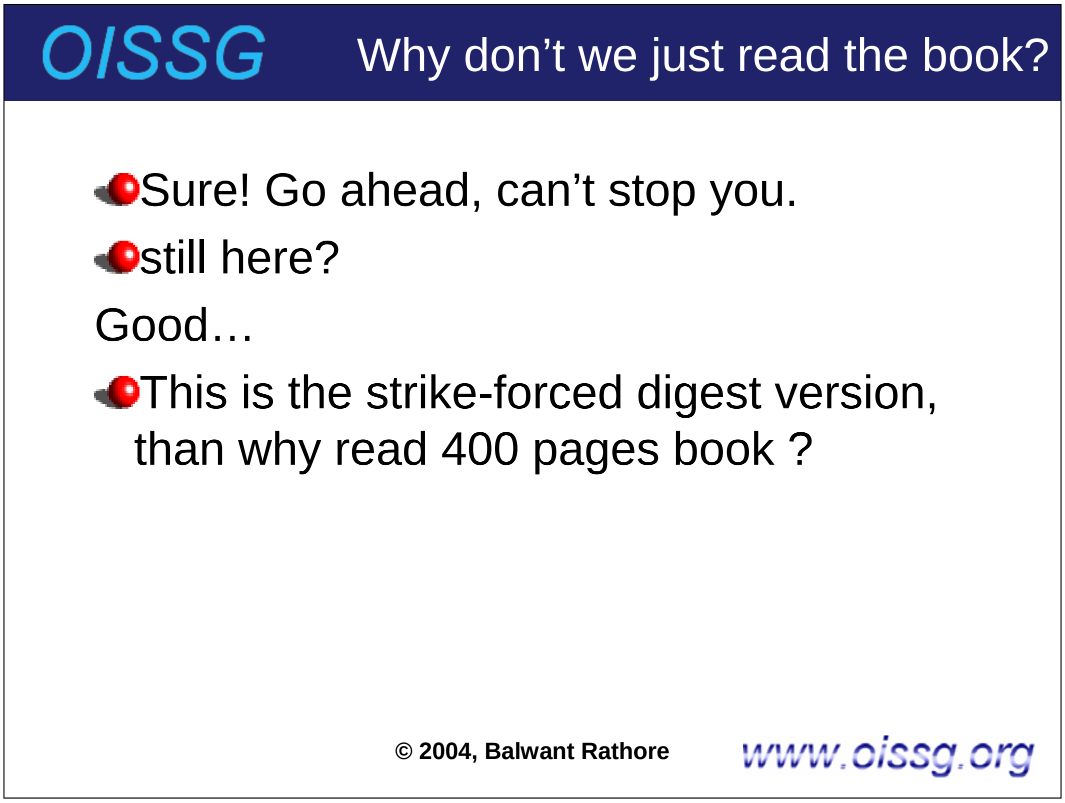


OISSG

What is this Presentation All About?

- This presentation is a technical summation of TCP/IP Protocol suit.
- This is targeted towards beginners in the field of information security.
- The presentation covers must know of TCP/IP from Security perspective.
- Forming a necessary technical base for Security professionals

www.oissg.org



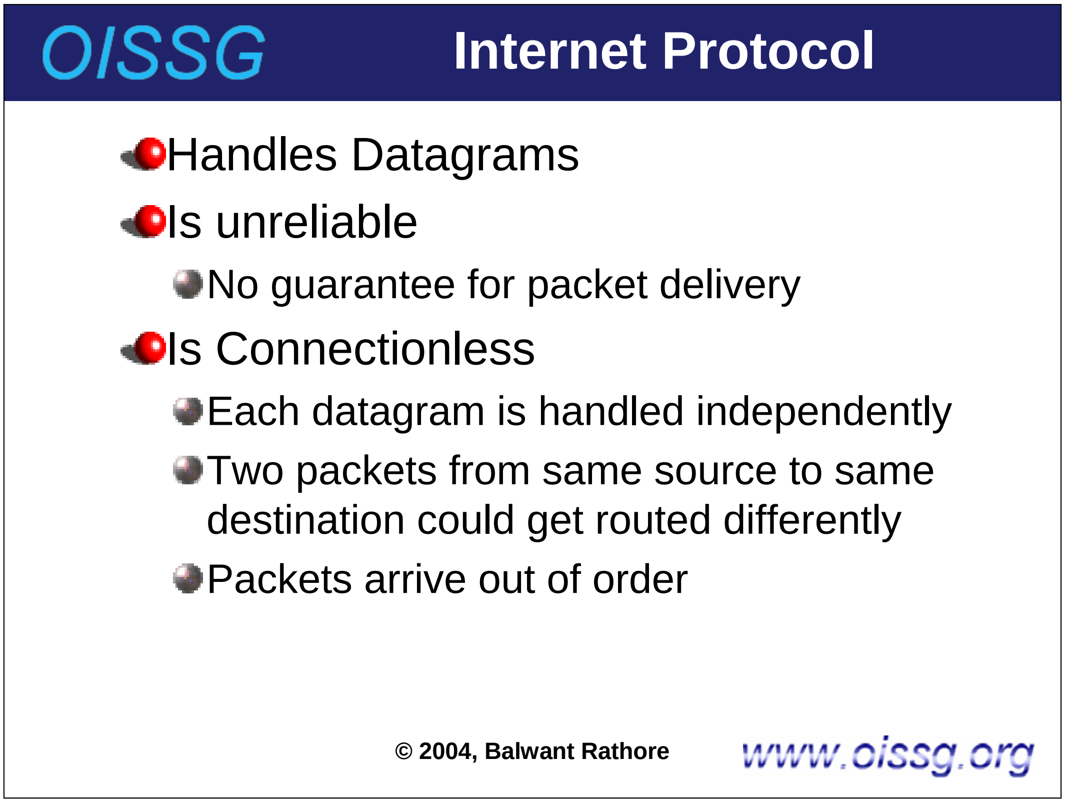
OISSG

Why don't we just read the book?

- Sure! Go ahead, can't stop you.
- still here?

Good…

- This is the strike-forced digest version, than why read 400 pages book ?



OISSG

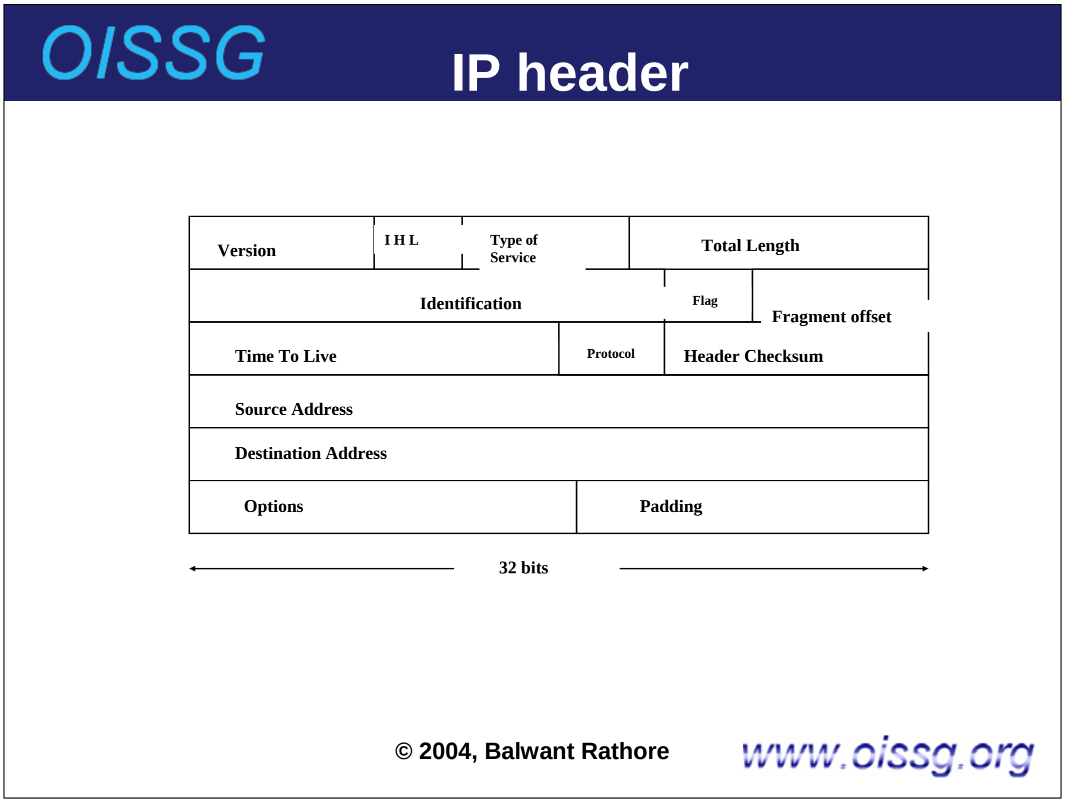
Internet Protocol

- Handles Datagrams
- Is unreliable
  - No guarantee for packet delivery
- Is Connectionless
  - Each datagram is handled independently
  - Two packets from same source to same destination could get routed differently
  - Packets arrive out of order

www.oissg.org

TCP/IP is the most widely used protocol suite today, which was developed under the sponsorship from DARPA (Defense Advanced Research Projects Agency). It is the de facto standard employed to interconnect computing facilities in modern network environments.

IP (Internet Protocol) is the workhorse protocol of the TCP/IP protocol suite, which provides an unreliable, connectionless datagram delivery service. All TCP, UDP(User Datagram Protocol), ICMP(Internet Control Message Protocol), and IGMP(Internet Group Management Protocol) data are transmitted as IP datagrams.



OISSG

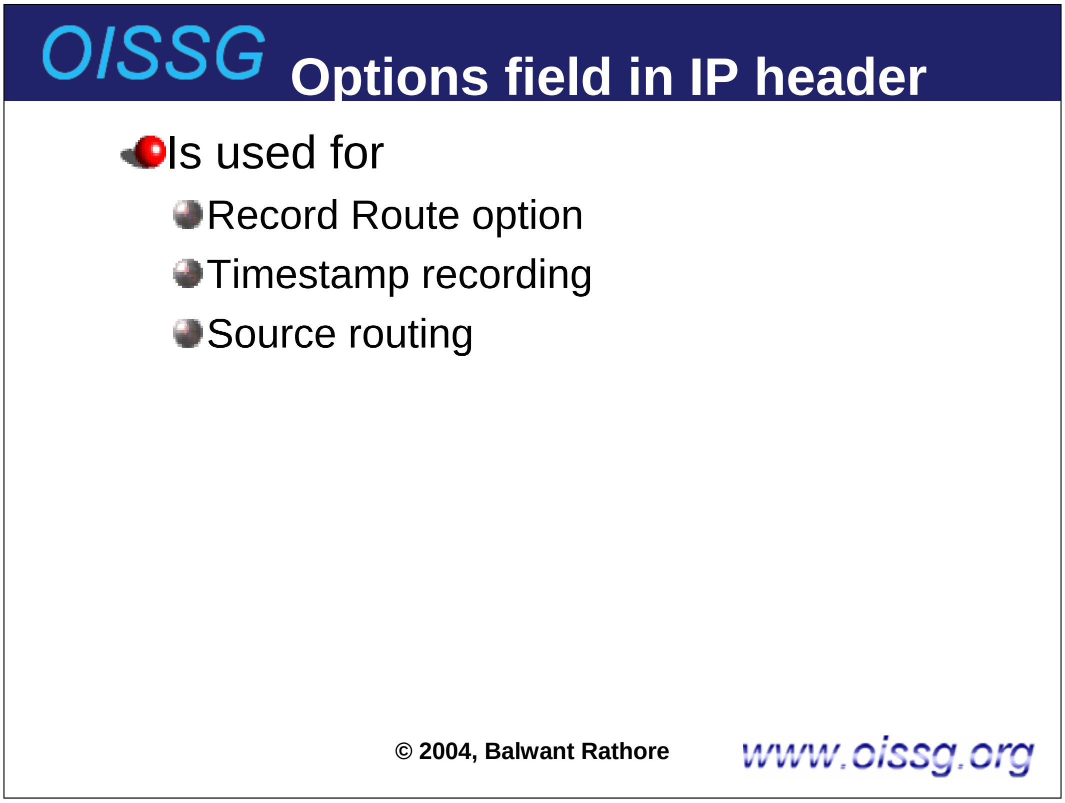
IP header

Version	I H L	Type of Service	Total Length
Identification	Flag	Fragment offset	
Time To Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options	Padding		

32 bits

www.oissg.org

Within IP header, there is important information like source IP address, destination IP address, which plays an important role in routing the packet around the network.



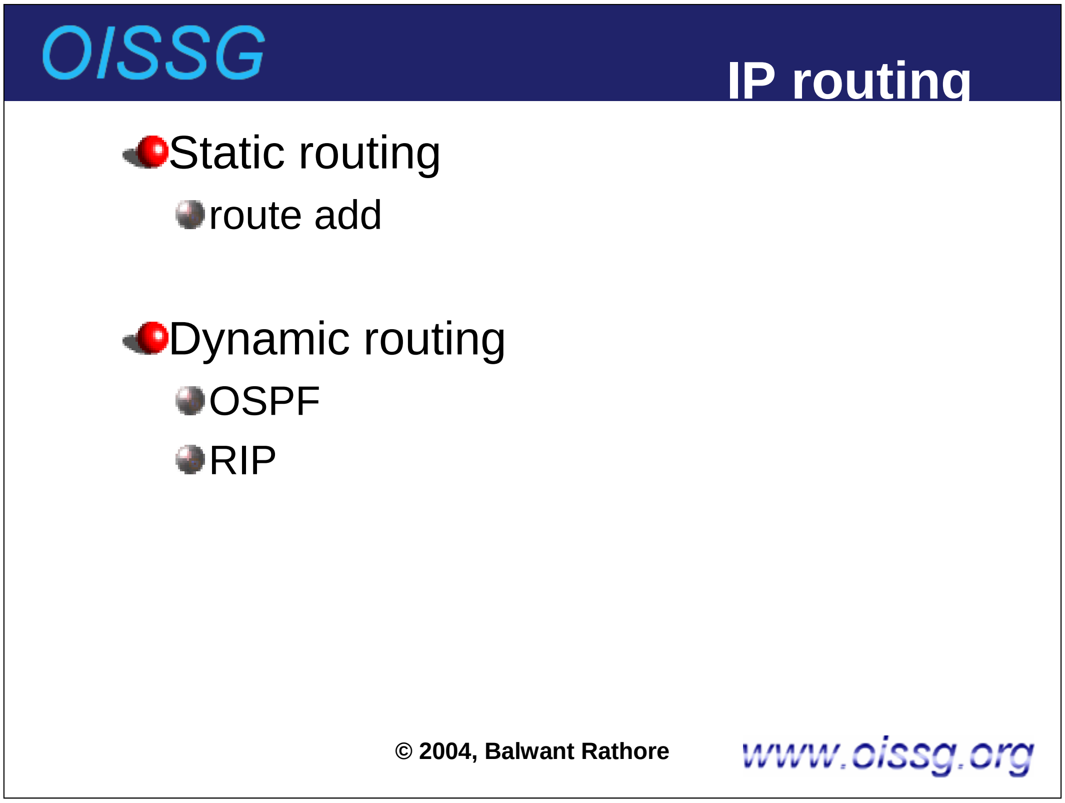
OISSG

Options field in IP header

- Is used for
  - Record Route option
  - Timestamp recording
  - Source routing

www.oissg.org

The Option fields in IP Header.



OISSG

IP routing

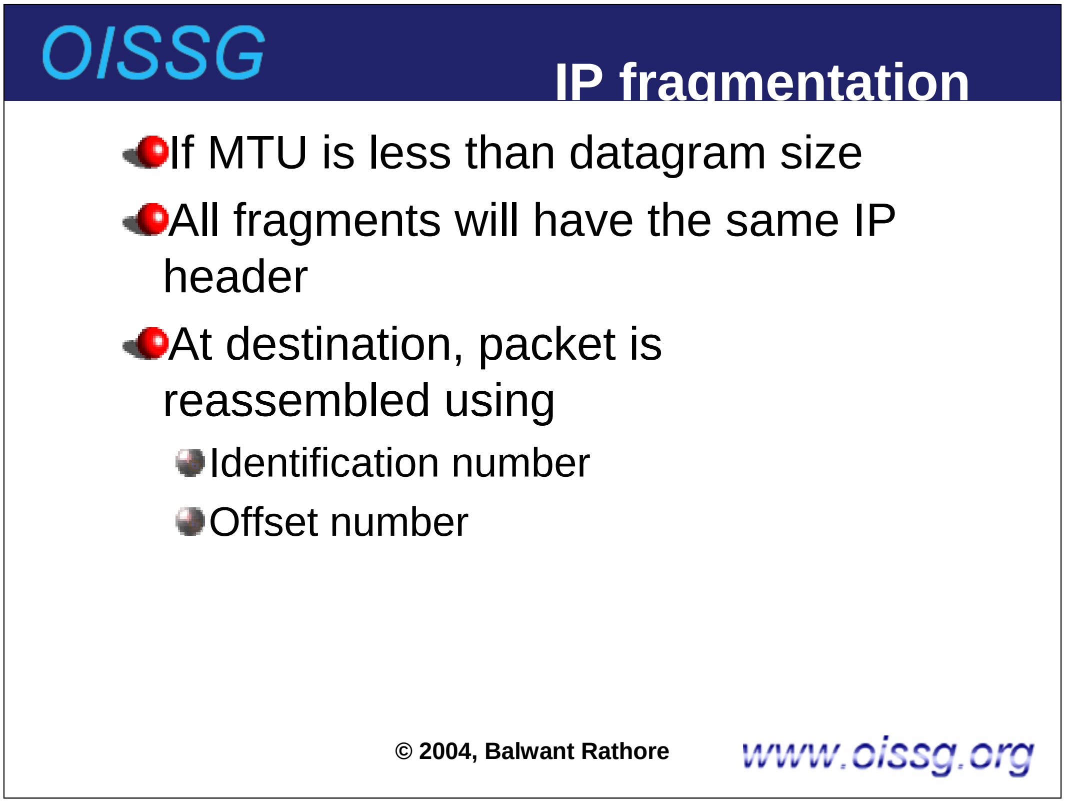
- Static routing
  - route add
- Dynamic routing
  - OSPF
  - RIP

www.oissg.org

IP Routing is of two types:

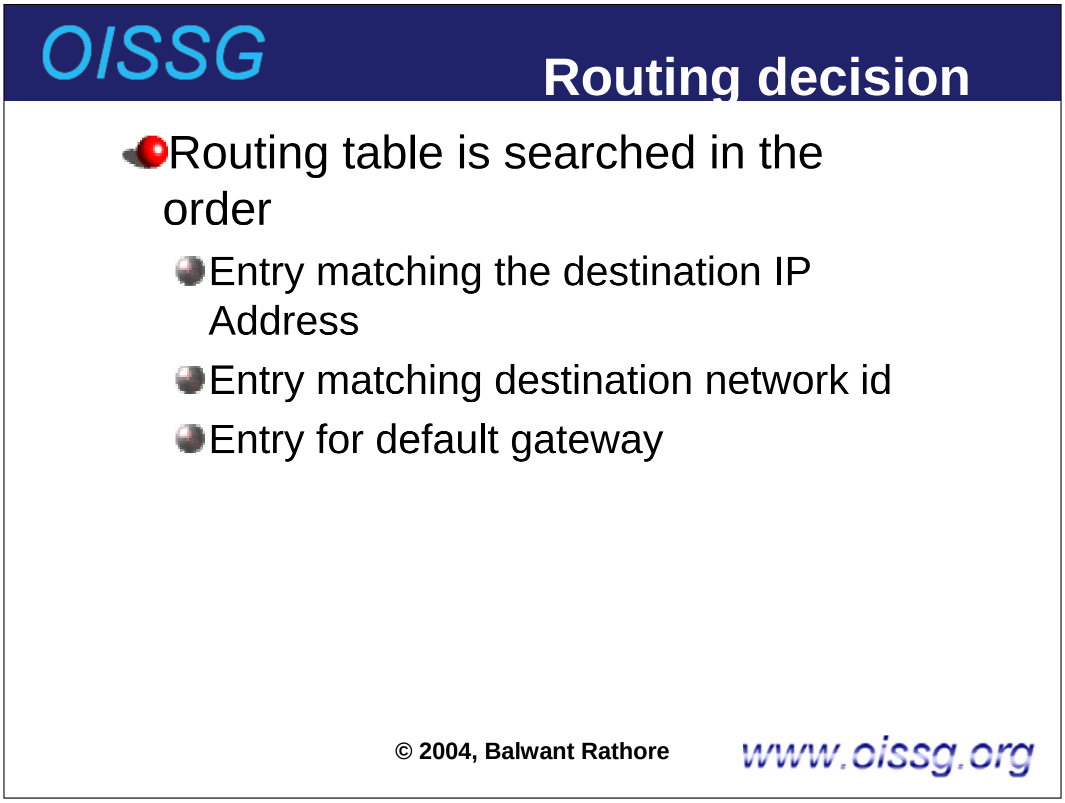
1. Static

2. Dynamic



IP fragmentation

- If MTU is less than datagram size
- All fragments will have the same IP header
- At destination, packet is reassembled using
  - Identification number
  - Offset number



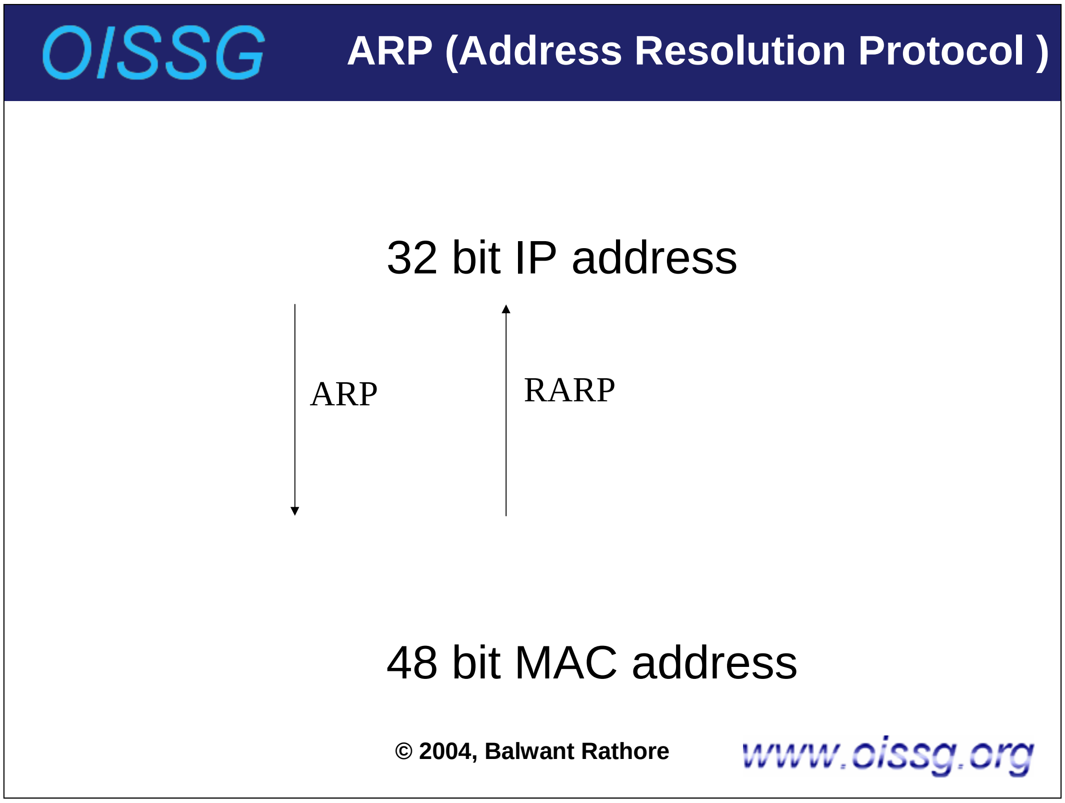
OISSG

Routing decision

- Routing table is searched in the order
  - Entry matching the destination IP Address
  - Entry matching destination network id
  - Entry for default gateway

www.oissg.org

The order in which the routing table is being searched for matching the IP, Network Id and the default gateway.



OISSG

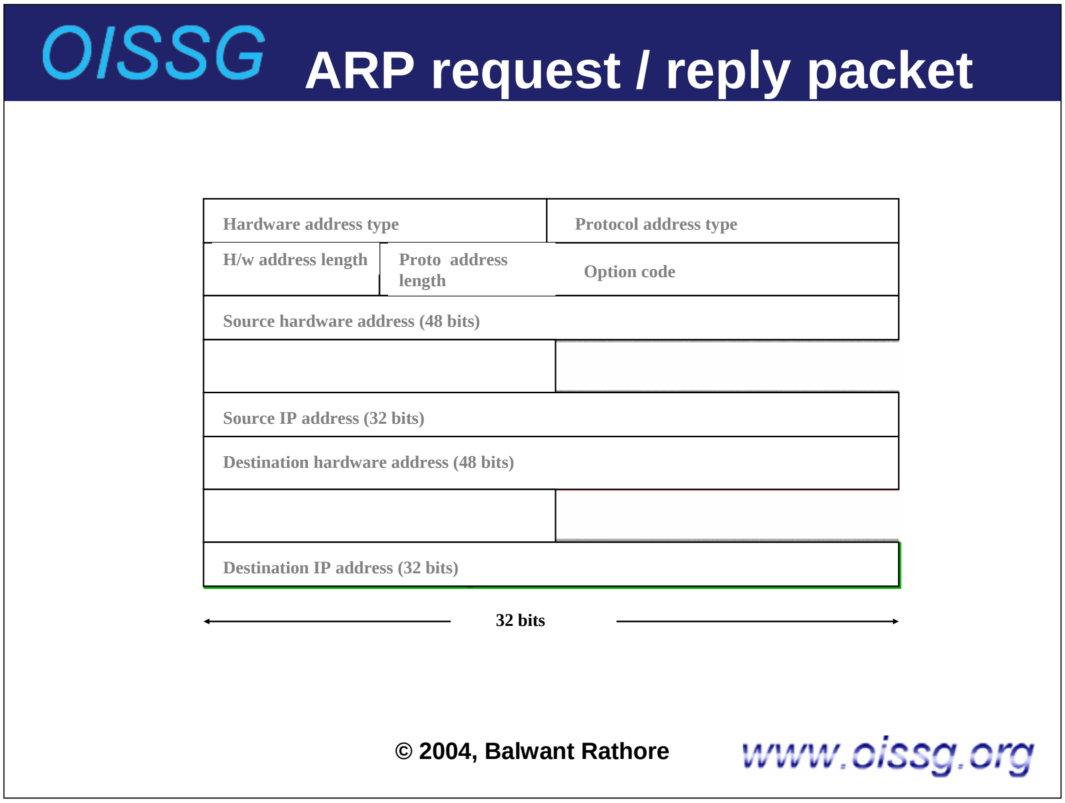
ARP (Address Resolution Protocol)

32 bit IP address

ARP

RARP

48 bit MAC address



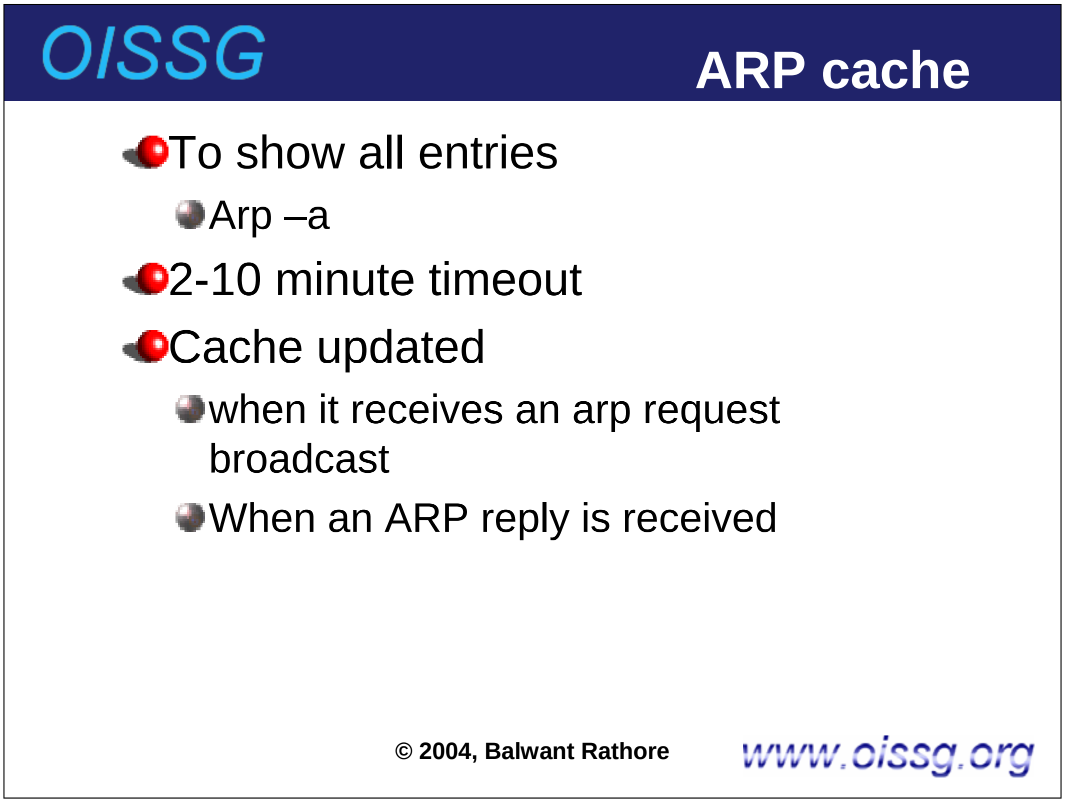
OISSG

ARP request / reply packet

Hardware address type		Protocol address type
H/w address length	Proto address length	Option code
Source hardware address (48 bits)		
Source IP address (32 bits)		
Destination hardware address (48 bits)		
Destination IP address (32 bits)		

← 32 bits →

www.oissg.org



OISSG

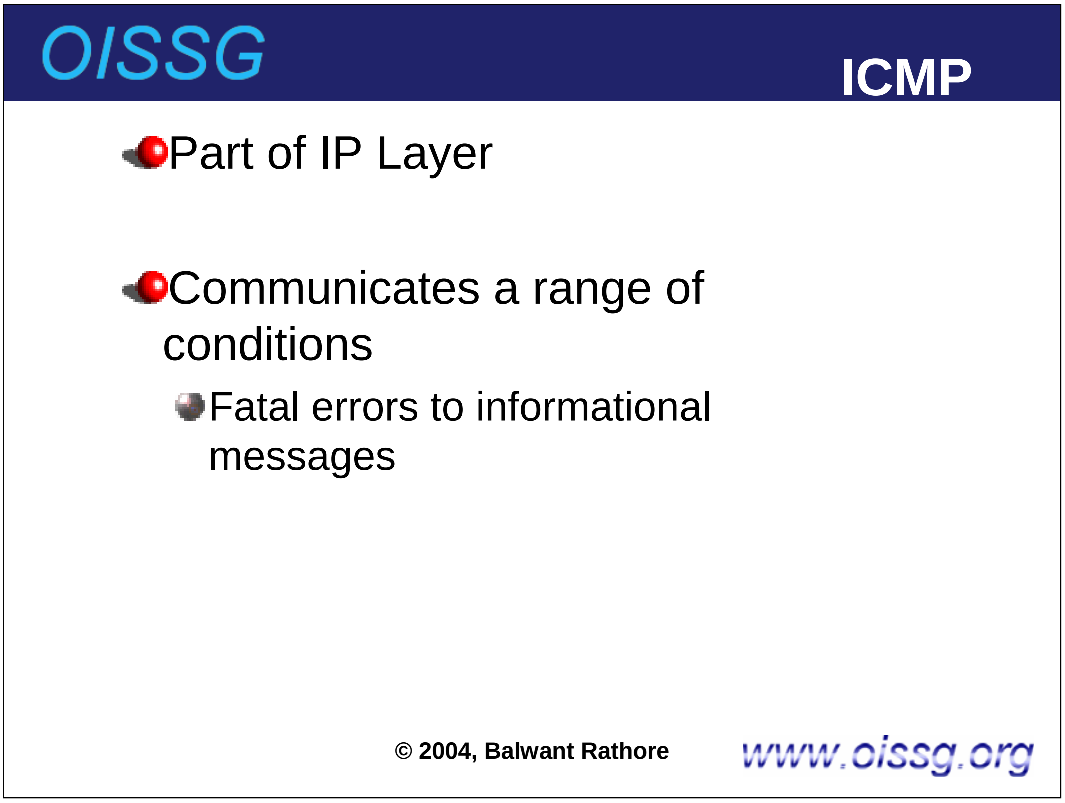
ARP cache

- To show all entries
  - Arp –a
- 2-10 minute timeout
- Cache updated
  - when it receives an arp request broadcast
  - When an ARP reply is received

www.oissg.org

More on ARP

- Proxy ARP
  - Answer ARP request on behalf of another host
  - Used to hide a set of hosts behind one IP
- Gratuitous ARP
  - Host sends ARP request for its own IP Address
  - Can detect IP address conflict

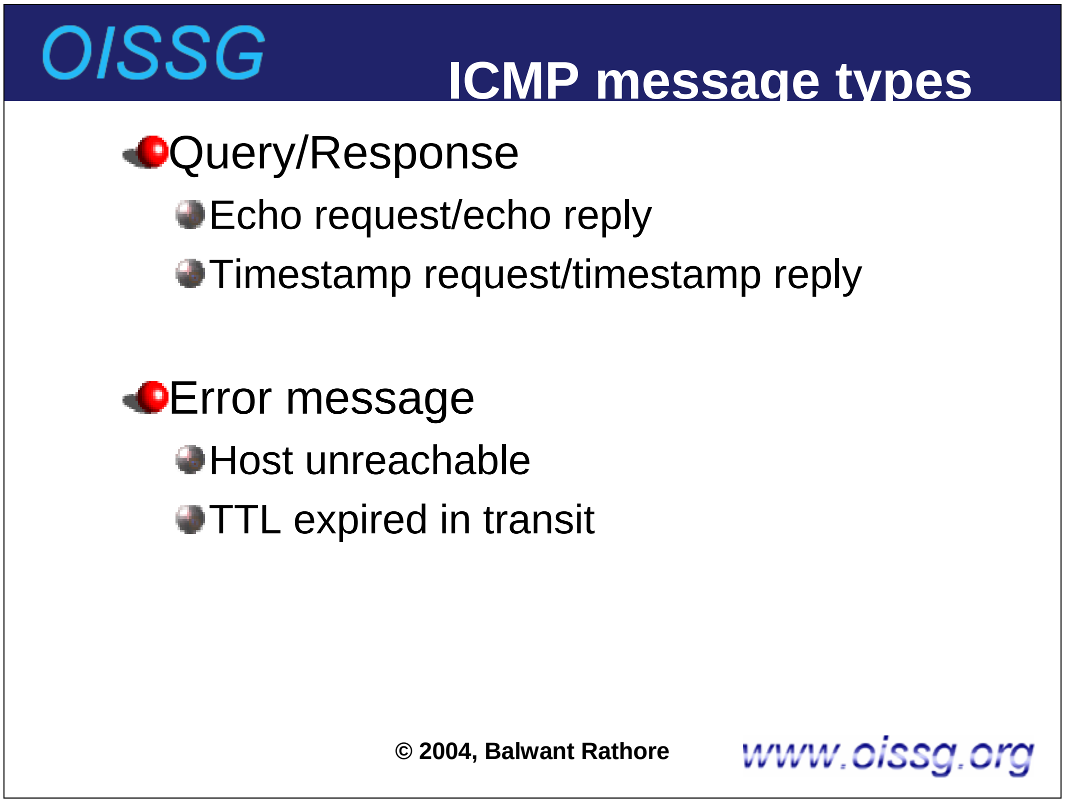


OISSG

ICMP

- Part of IP Layer
- Communicates a range of conditions
  - Fatal errors to informational messages

www.oissg.org



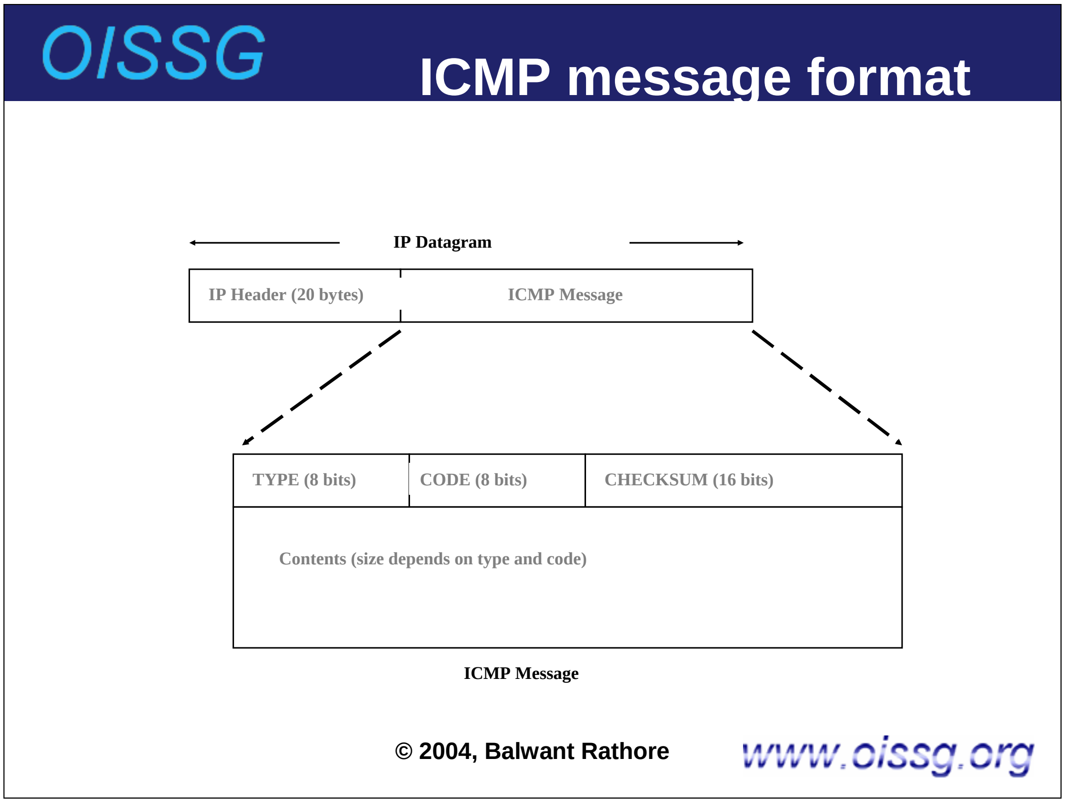
OISSG

ICMP message types

- Query/Response
  - Echo request/echo reply
  - Timestamp request/timestamp reply
- Error message
  - Host unreachable
  - TTL expired in transit

www.oissg.org

ICMP either send the query response or the error message



OISSG

ICMP message format

IP Datagram

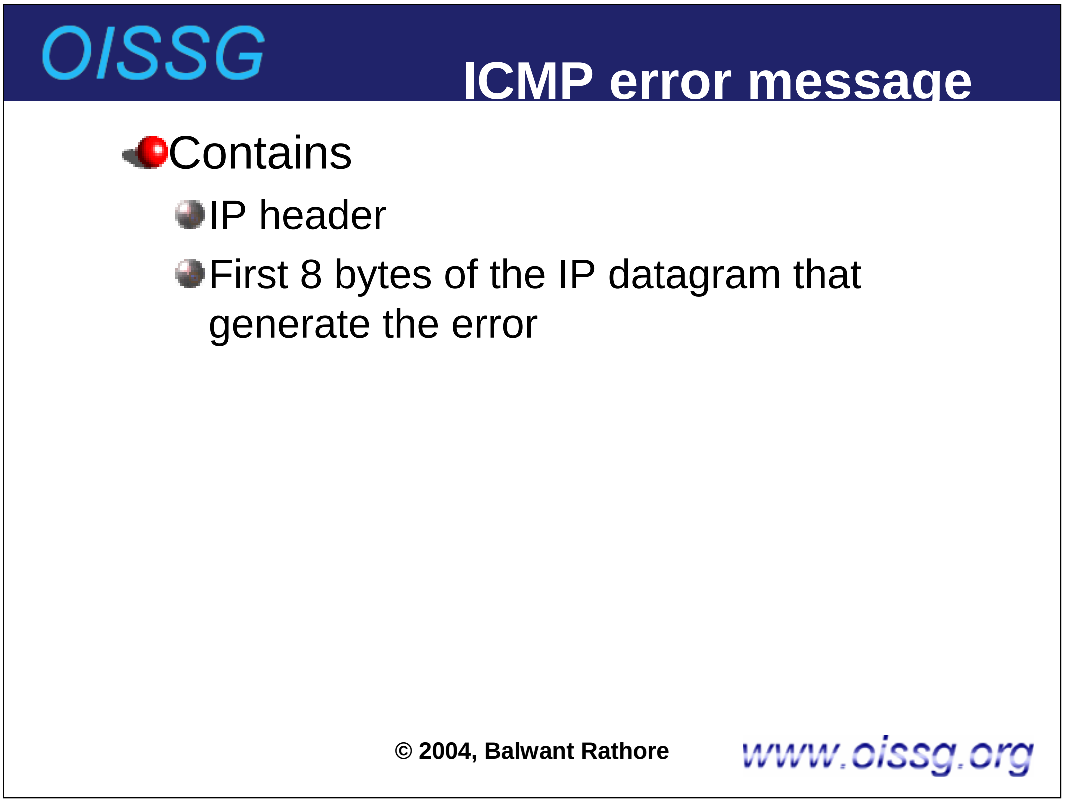
IP Header (20 bytes) | ICMP Message

TYPE (8 bits)	CODE (8 bits)	CHECKSUM (16 bits)
Contents (size depends on type and code)		

ICMP Message

www.oissg.org

A typical ICMP message format.



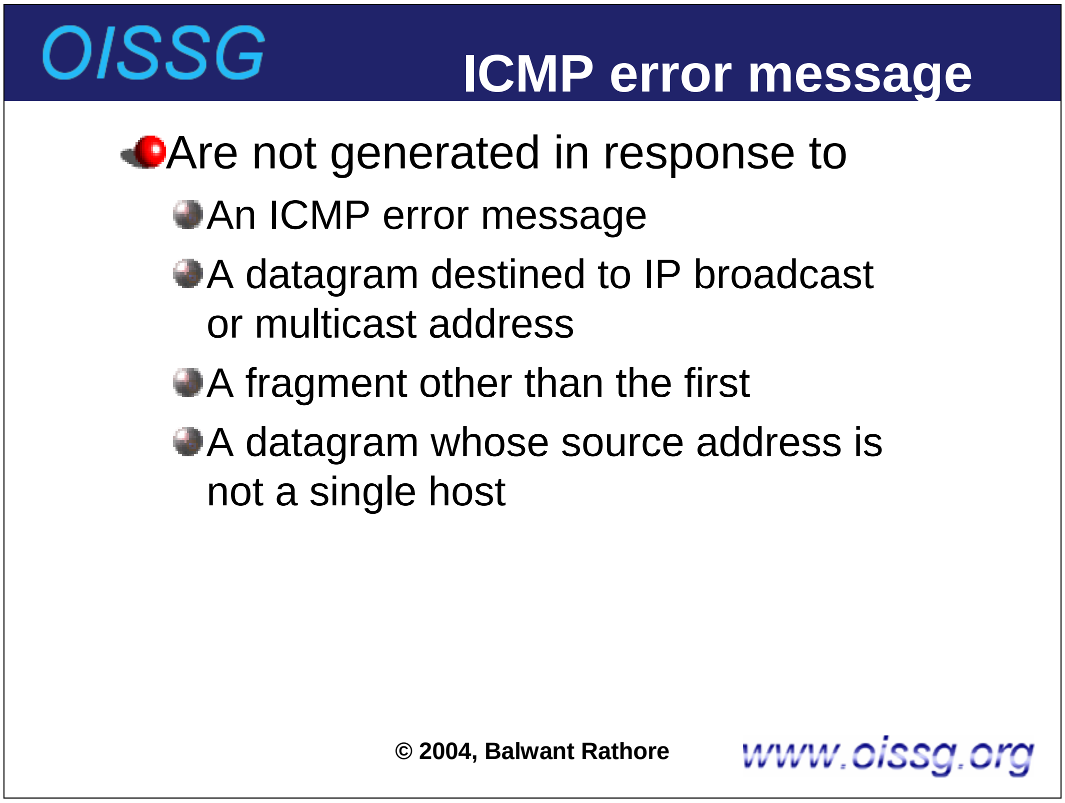
OISSG

ICMP error message

- Contains
  - IP header
  - First 8 bytes of the IP datagram that generate the error

www.oissg.org

An ICMP error message contains the following: IP Header and First 8 bytes of the IP datagram that generates the error



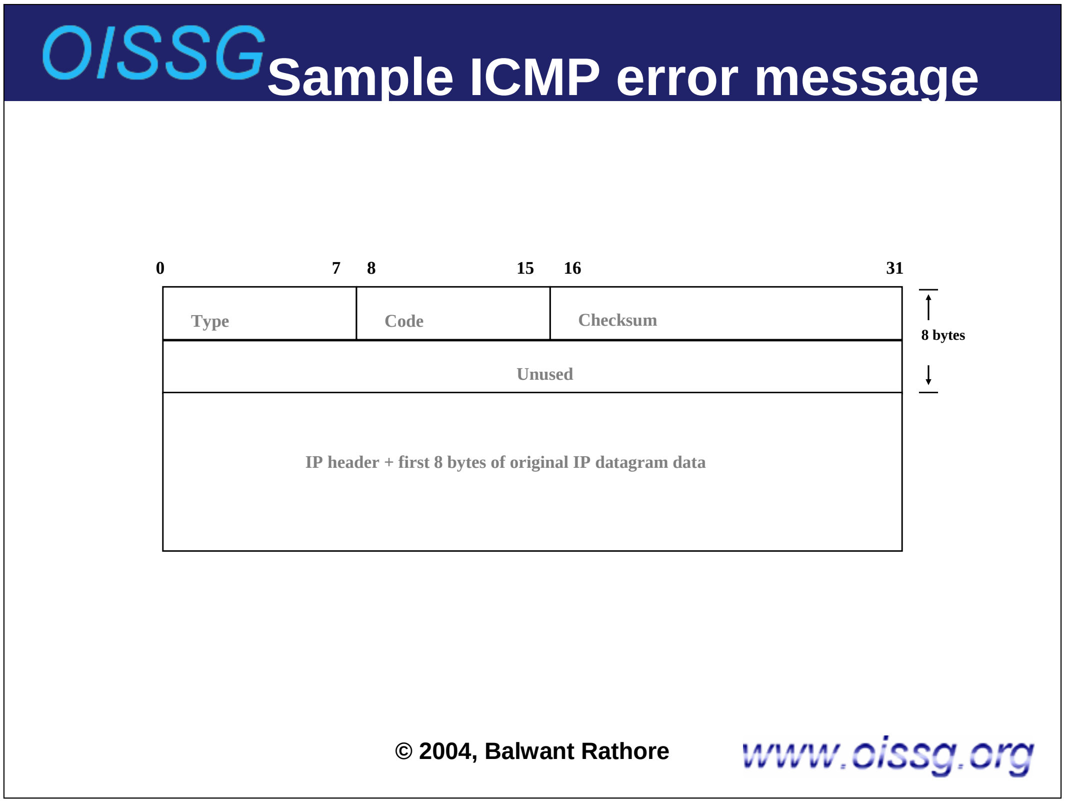
OISSG

ICMP error message

- Are not generated in response to
  - An ICMP error message
  - A datagram destined to IP broadcast or multicast address
  - A fragment other than the first
  - A datagram whose source address is not a single host

www.oissg.org

ICMP Error Message Quoting Size: All ICMP error messages consist of an IP header, an ICMP header and certain amount of data of the original datagram, which triggered the error (also known as offending datagram). According to RFC 792 only 64 bits (8 octets) of original datagram are supposed to be included in the ICMP error message. However RFC 1122 (issued later) recommends up to 576 octets to be quoted.



OISSG

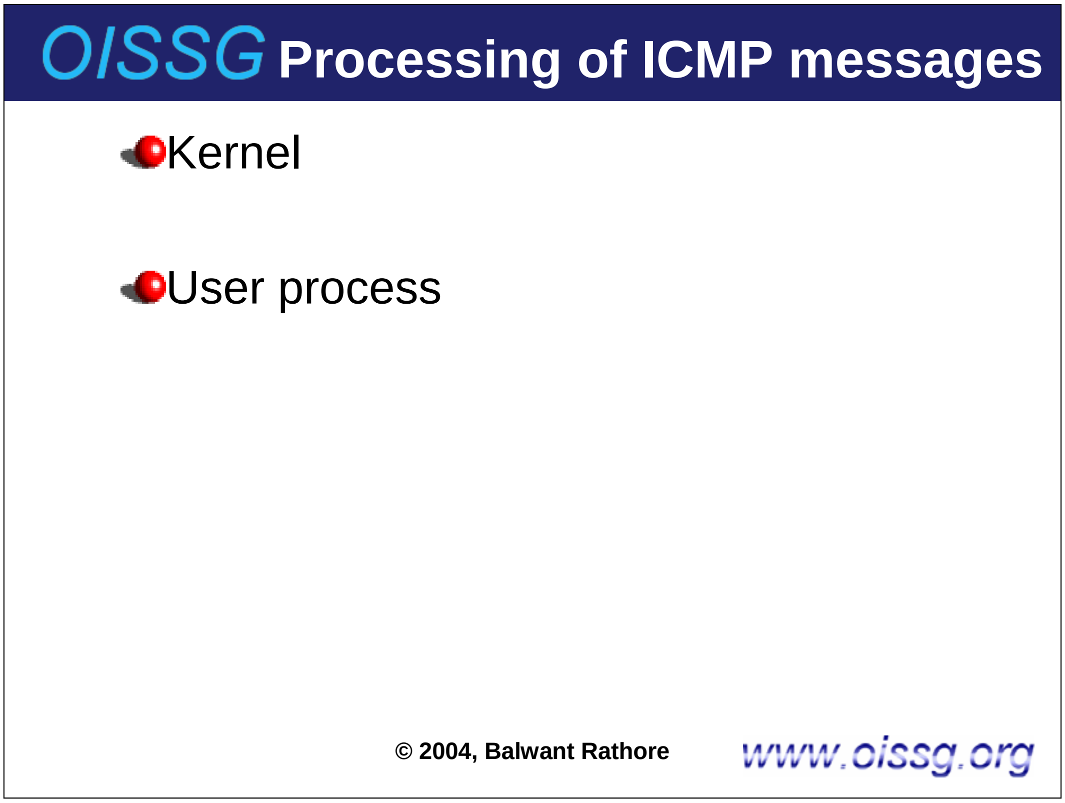
Sample ICMP error message

0 – 7	8 – 15	16 – 31
Type	Code	Checksum
Unused		
IP header + first 8 bytes of original IP datagram data		

8 bytes

www.oissg.org

Sample ICMP error message with format

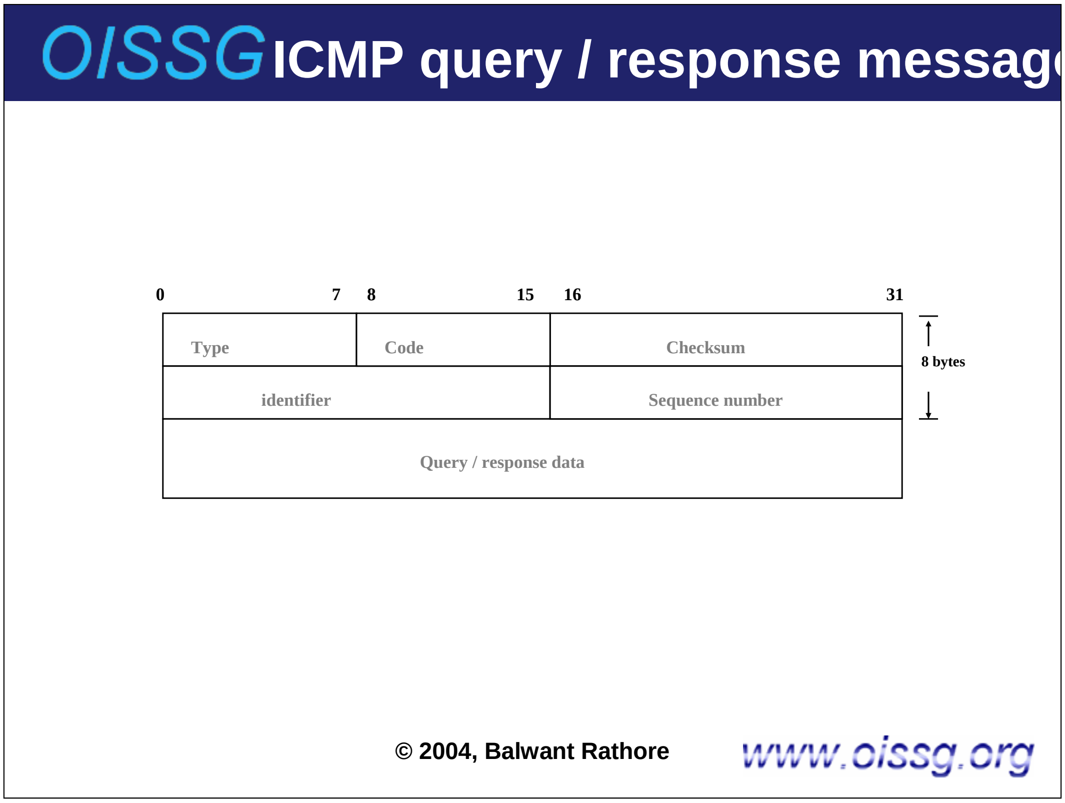


OISSG Processing of ICMP messages

- Kernel
- User process

www.oissg.org

Linux Kernel 2.0.x, 2.2.x, 2.4.x will act as routers and will set their Precedence bits field value to 0xc0 with ICMP error messages. Networking devices that will act the same will be Cisco routers based on IOS 11.x-12.x and Foundry Networks switches.



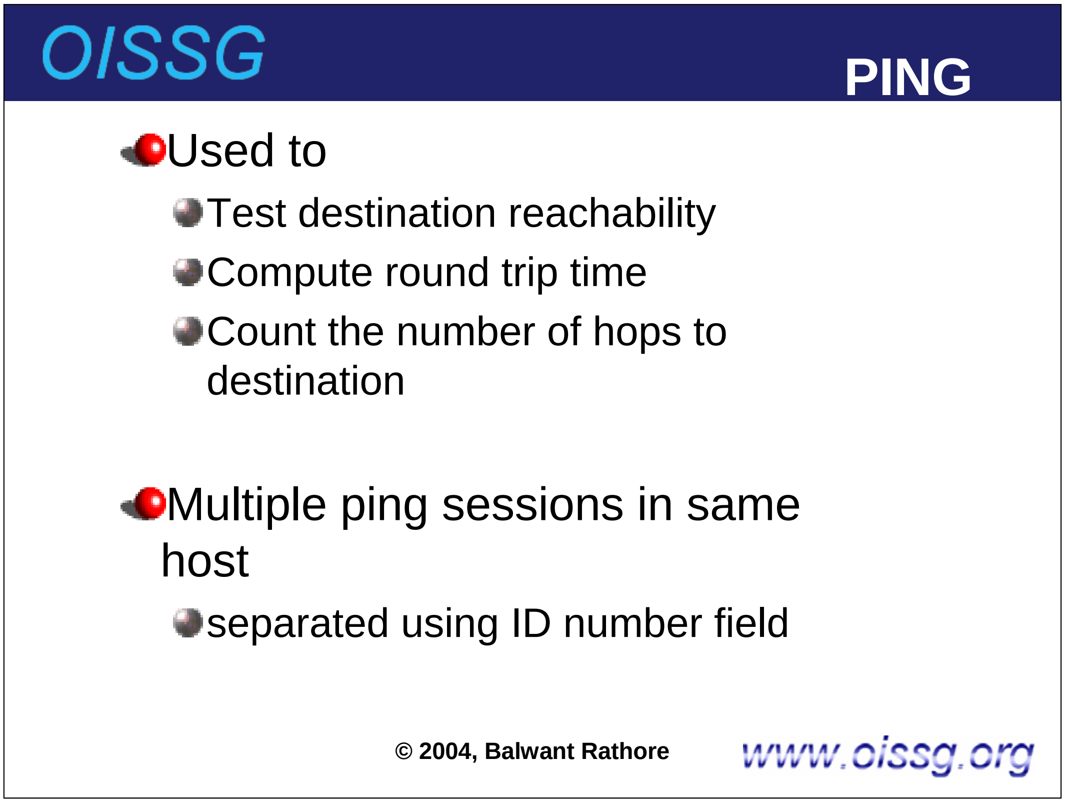
ICMP query / response messag

0 7	8 15	16 31
Type	Code	Checksum
identifier		Sequence number
Query / response data		

8 bytes

www.oissg.org

ICMP query / response message with format.



OISSG

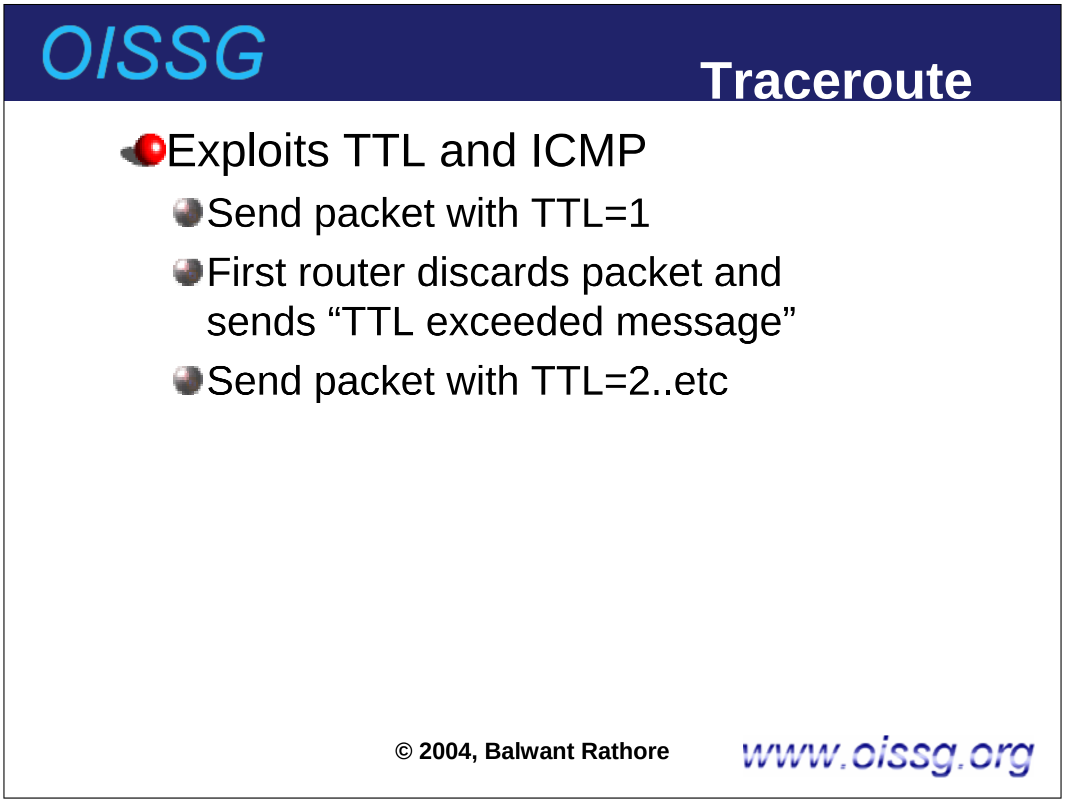
PING

- Used to
  - Test destination reachability
  - Compute round trip time
  - Count the number of hops to destination
- Multiple ping sessions in same host
  - separated using ID number field

© 2004, Balwant Rathore

www.oissg.org

Ping is may be the most known ICMP packet ICMP ECHO REQUEST (type 8) and the reply is ICMP ECHO REPLY (type 0). Therefore most firewall admin blocks incoming pings, however they do not care about other types of ICMP packets, which can be handy for gathering juicy information from the target.



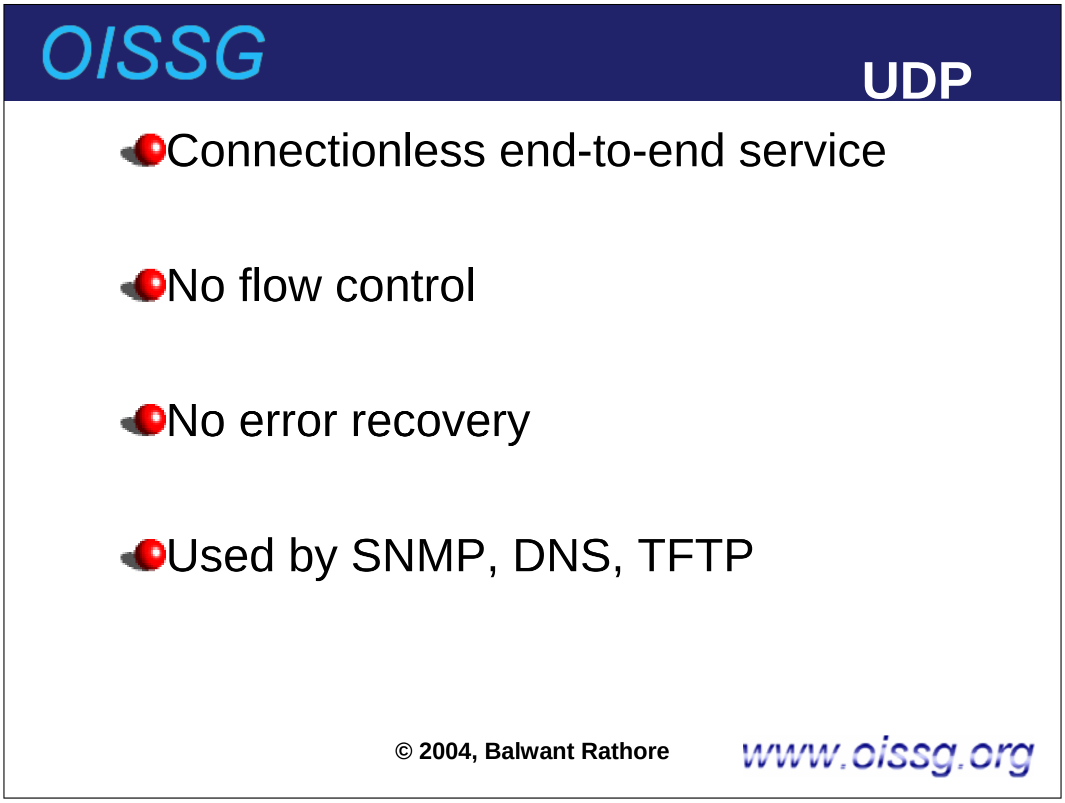
OISSG

Traceroute

- Exploits TTL and ICMP
  - Send packet with TTL=1
  - First router discards packet and sends “TTL exceeded message”
  - Send packet with TTL=2..etc

www.oissg.org

Traceroute is a network debugging utility, which attempts to map all the hosts on a route to a certain destination host/machine. It sends UDP datagrams by default or ICMP ECHO Request packets with TTL (time to live) fields set to 1 just before reaching the final target. Once the target reached, as TTL field gets zero, the target will discard the datagram and generate an ICMP Time Exceeded packet back to its originator. By the way, Windows systems use ICMP ECHO Request by default and you can not use UDP method with Microsoft’s traceroute implementation, "tracert".



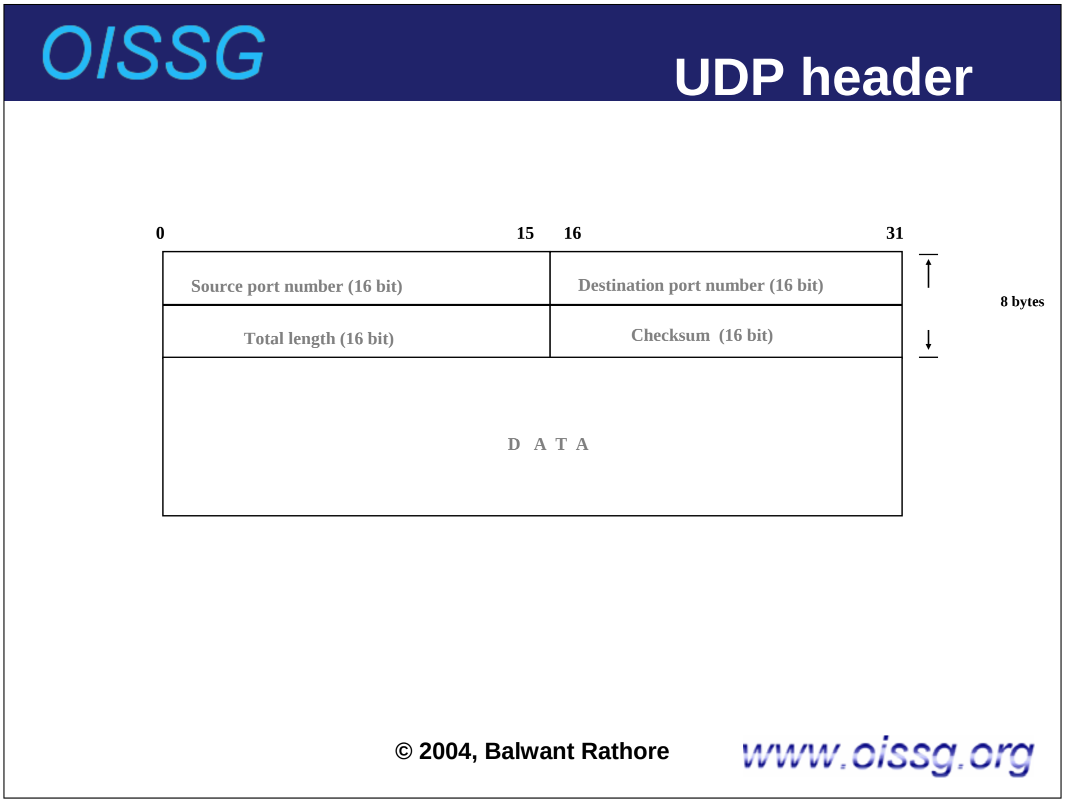
OISSG

UDP

- Connectionless end-to-end service
- No flow control
- No error recovery
- Used by SNMP, DNS, TFTP

www.oissg.org

UDP is a transportation layer protocol, but it does not offer much more functionality other than IP. The checksum field in UDP header provides only a limited ability for error checking.



OISSG

UDP header

0 15	16 31	
Source port number (16 bit)	Destination port number (16 bit)	8 bytes
Total length (16 bit)	Checksum (16 bit)	
DATA		

© 2004, Balwant Rathore

www.oissg.org

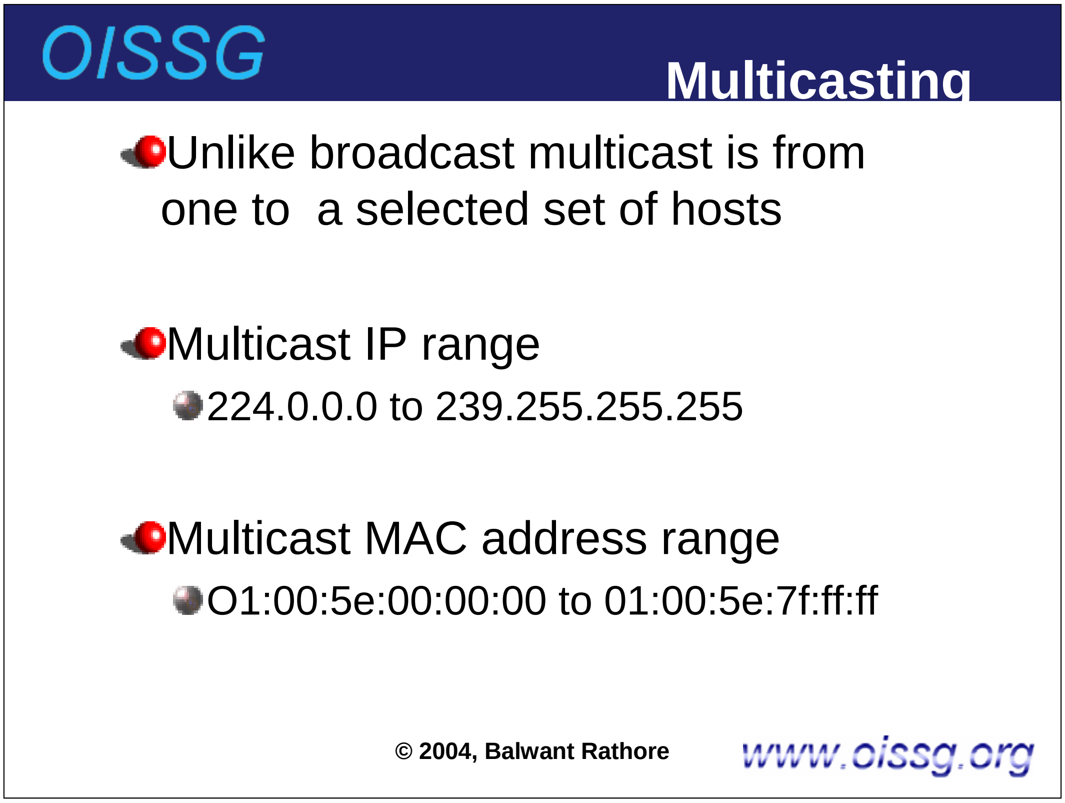
However, due to its simplicity and less overhead comparing with connection-oriented protocols, UDP is suitable for the design of simple request/reply application, such as DNS(Domain Name System), SNMP(Simple Network Management Protocol) and database transaction.

OISSG

Broadcast

- Limited Broadcast
  - 255.255.255.255
- Net directed broadcast
  - 202.54.13.255
- Broadcast MAC Address
  - Always ff:ff:ff:ff:ff:ff

www.oissg.org

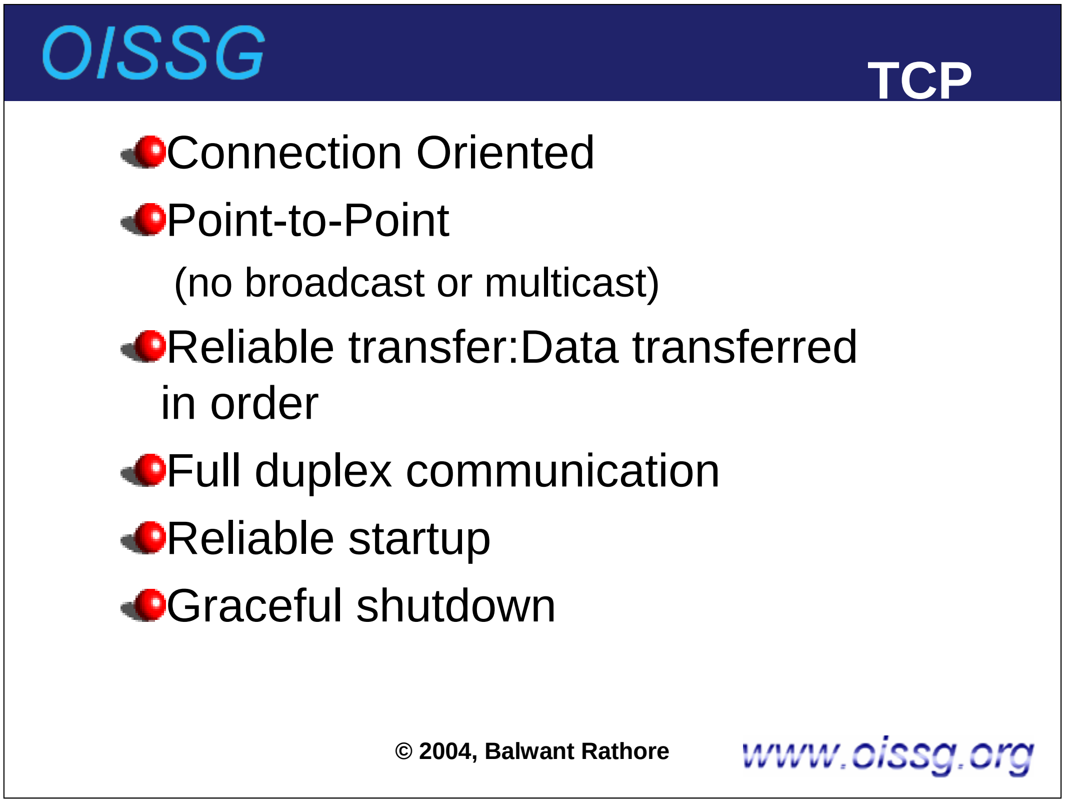


OISSG

Multicasting

- Unlike broadcast multicast is from one to a selected set of hosts
- Multicast IP range
  - 224.0.0.0 to 239.255.255.255
- Multicast MAC address range
  - O1:00:5e:00:00:00 to 01:00:5e:7f:ff:ff

www.oissg.org



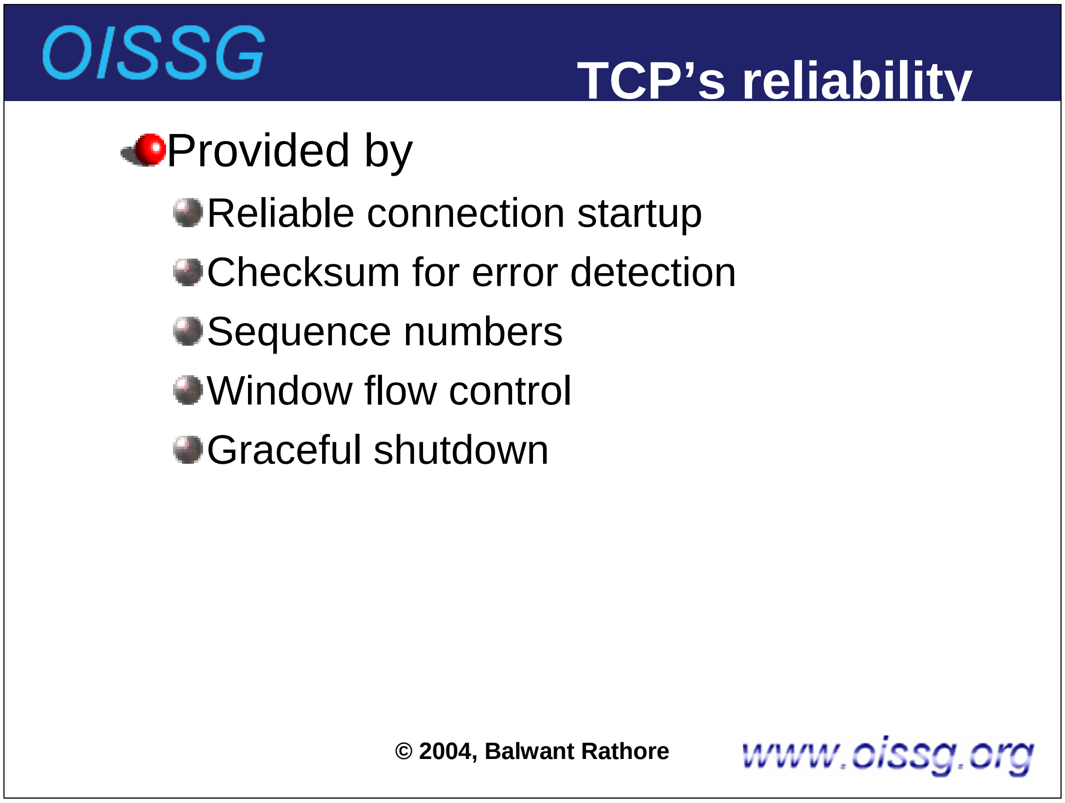
OISSG

TCP

- Connection Oriented
- Point-to-Point
  (no broadcast or multicast)
- Reliable transfer:Data transferred in order
- Full duplex communication
- Reliable startup
- Graceful shutdown

www.oissg.org

TCP is built on top of IP layer, which is unreliable and connectionless. However, TCP provides higher layer application a reliable connection-oriented service. As a tradeoff, each TCP connection requires an establishment procedure and a termination step between communication peers. Furthermore, TCP also provides sequencing and flow control which are helpful in transmission of packets.



OISSG

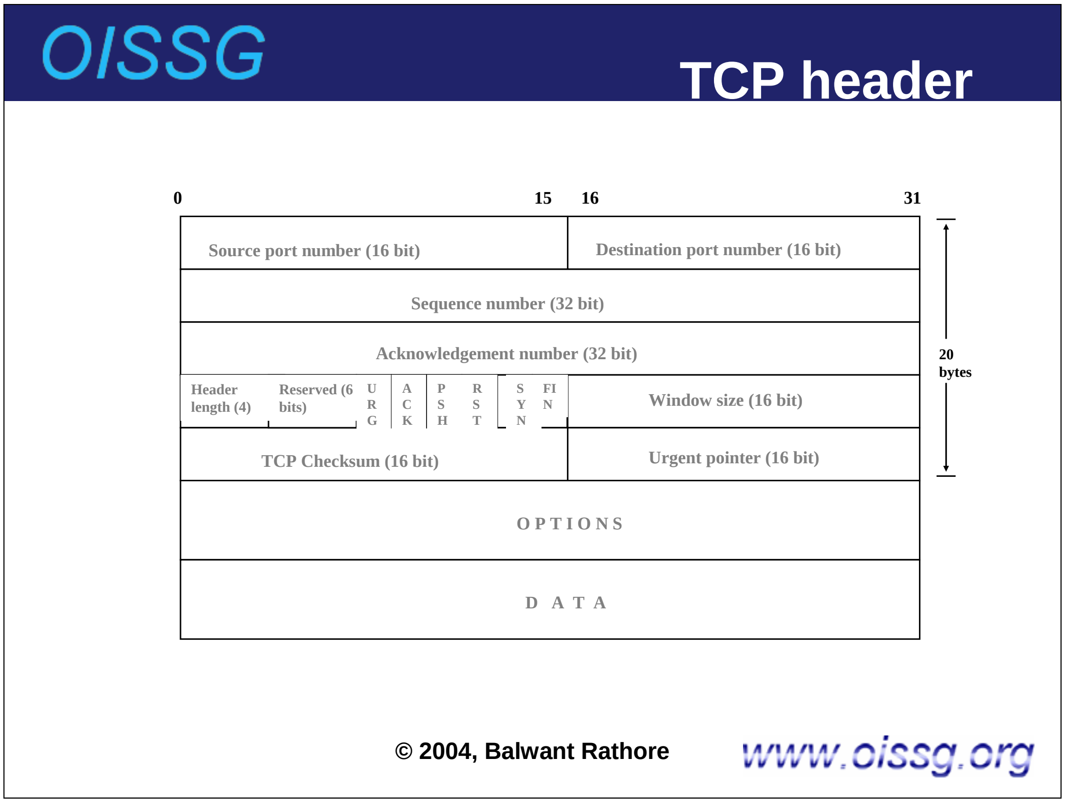
TCP’s reliability

- Provided by
  - Reliable connection startup
  - Checksum for error detection
  - Sequence numbers
  - Window flow control
  - Graceful shutdown

www.oissg.org

TCP is reliable for the following:

- Reliable connection startup
- Checksum for error detection
- Sequence numbers
- Window flow control
- Graceful shutdown



OISSG

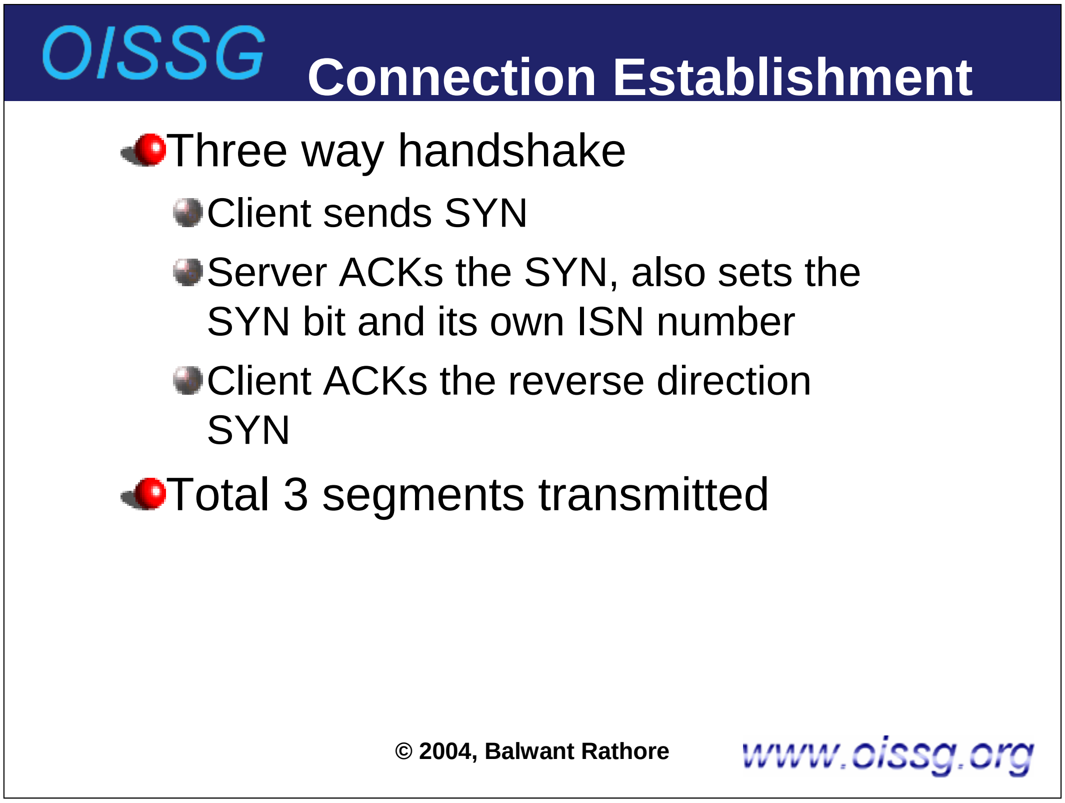
TCP header

0 15	16 31
Source port number (16 bit)	Destination port number (16 bit)
Sequence number (32 bit)	
Acknowledgement number (32 bit)	
Header length (4) Reserved (6 bits) URG ACK PSH RST SYN FIN	Window size (16 bit)
TCP Checksum (16 bit)	Urgent pointer (16 bit)
OPTIONS	
DATA	

20 bytes

www.oissg.org

Without options, TCP header occupies 20 bytes as shown in the figure. The source and destination port number is used to identify the sending and receiving processes. The sequence number is essential in keeping sent and received datagram in proper order. There are six flag bits with the TCP header, namely URG, ACK, PSH, RST, SYN and FIN, each of them has a special use in the connection establishment, connection termination or other control purposes. Window size is advertised between communication peers to maintain the flow control.



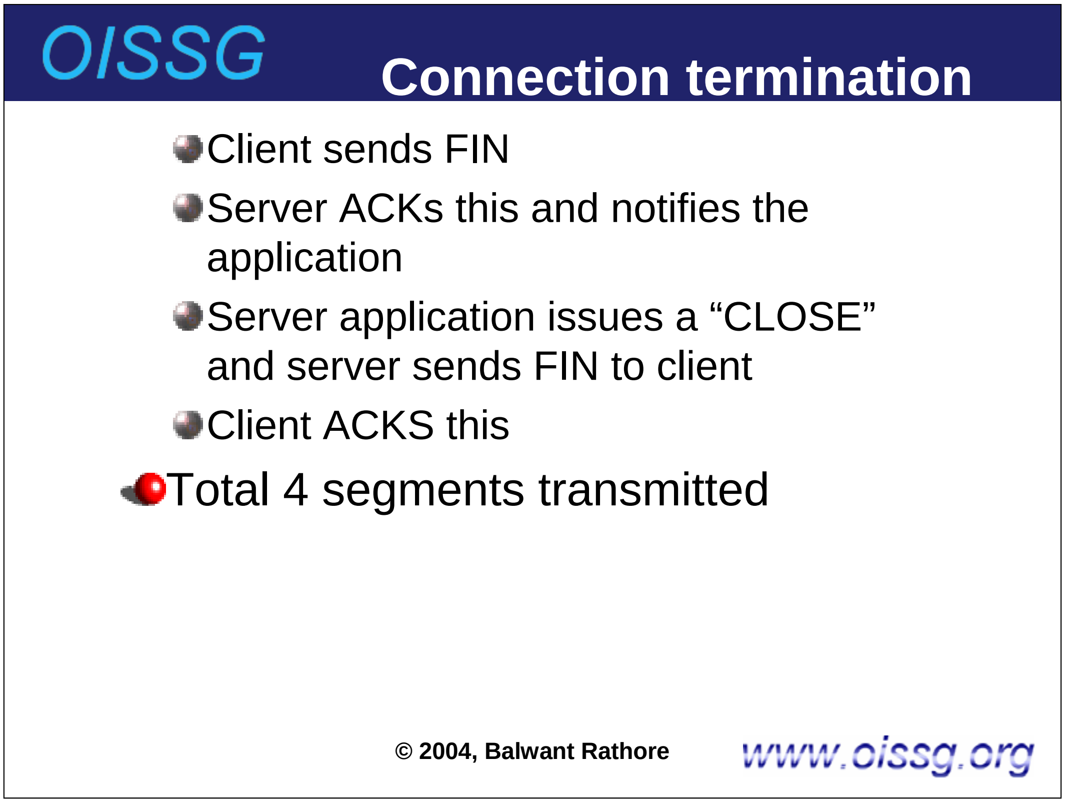
OISSG

Connection Establishment

- Three way handshake
  - Client sends SYN
  - Server ACKs the SYN, also sets the SYN bit and its own ISN number
  - Client ACKs the reverse direction SYN
- Total 3 segments transmitted

www.oissg.org

TCP establishes a connection in three steps, namely three-way handshake. It is a typical three-way handshake procedure happened between a source host S and a destination host D.



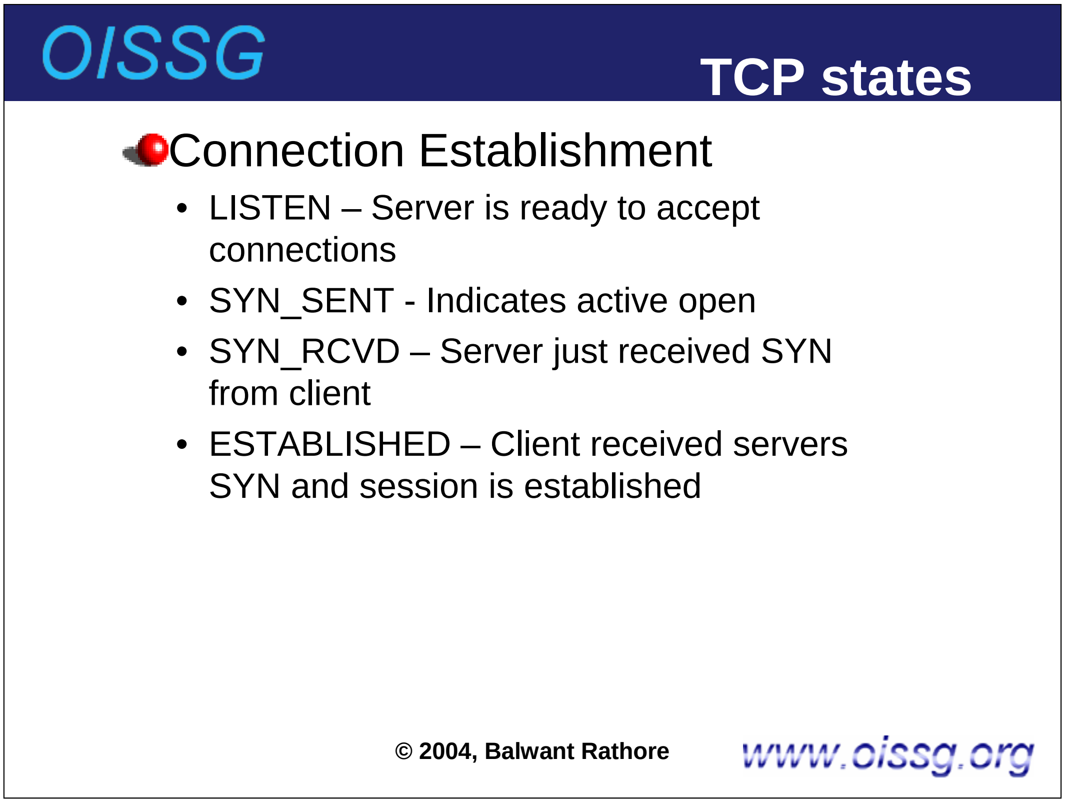
Connection termination

- Client sends FIN
- Server ACKs this and notifies the application
- Server application issues a “CLOSE” and server sends FIN to client
- Client ACKS this

- Total 4 segments transmitted

To terminate the connection following are the steps:

First the client sends the FIN packet/request, server also sends the acknowledgement packet/response to the client and than send the FIN packet/request to the client in order to close the connection. After getting the FIN from the server the client acknowledges this and the connection is finally terminated.



OISSG

TCP states

- Connection Establishment
  - LISTEN – Server is ready to accept connections
  - SYN_SENT - Indicates active open
  - SYN_RCVD – Server just received SYN from client
  - ESTABLISHED – Client received servers SYN and session is established

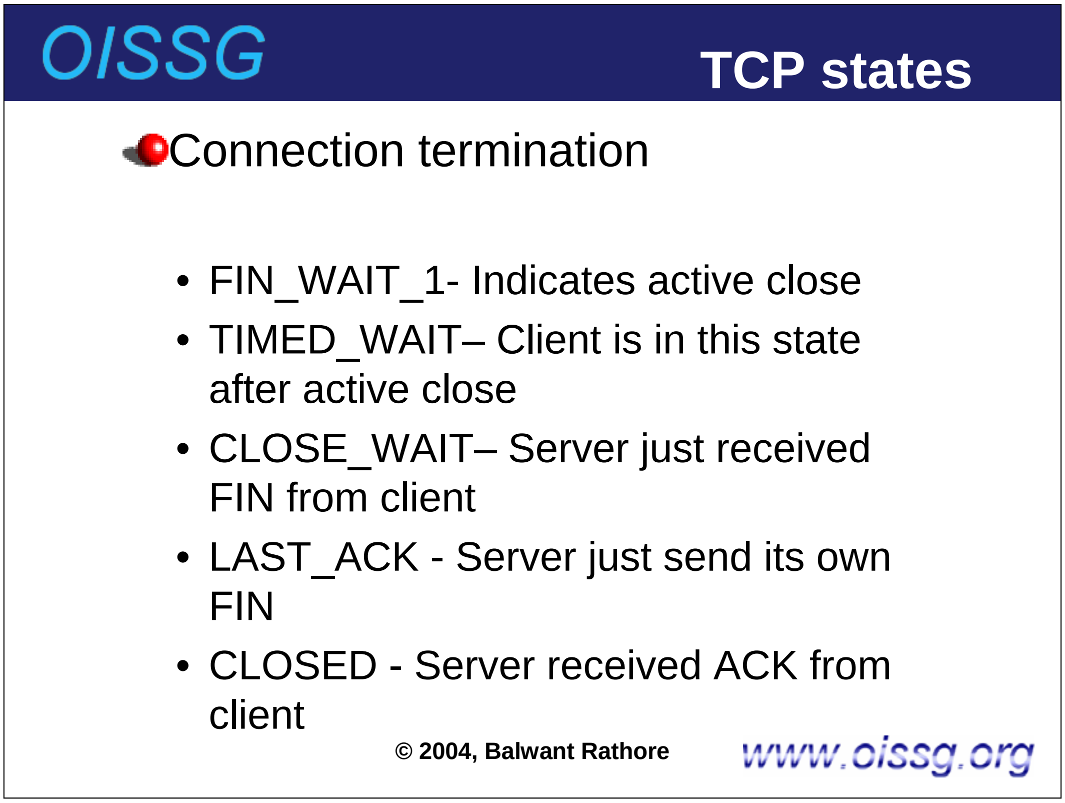
TCP States at the time of connection establishment:

LISTEN – Server is ready to accept connections

SYN_SENT - Indicates active open

SYN_RCVD – Server just received SYN from client

ESTABLISHED – Client received servers SYN and session is established



OISSG

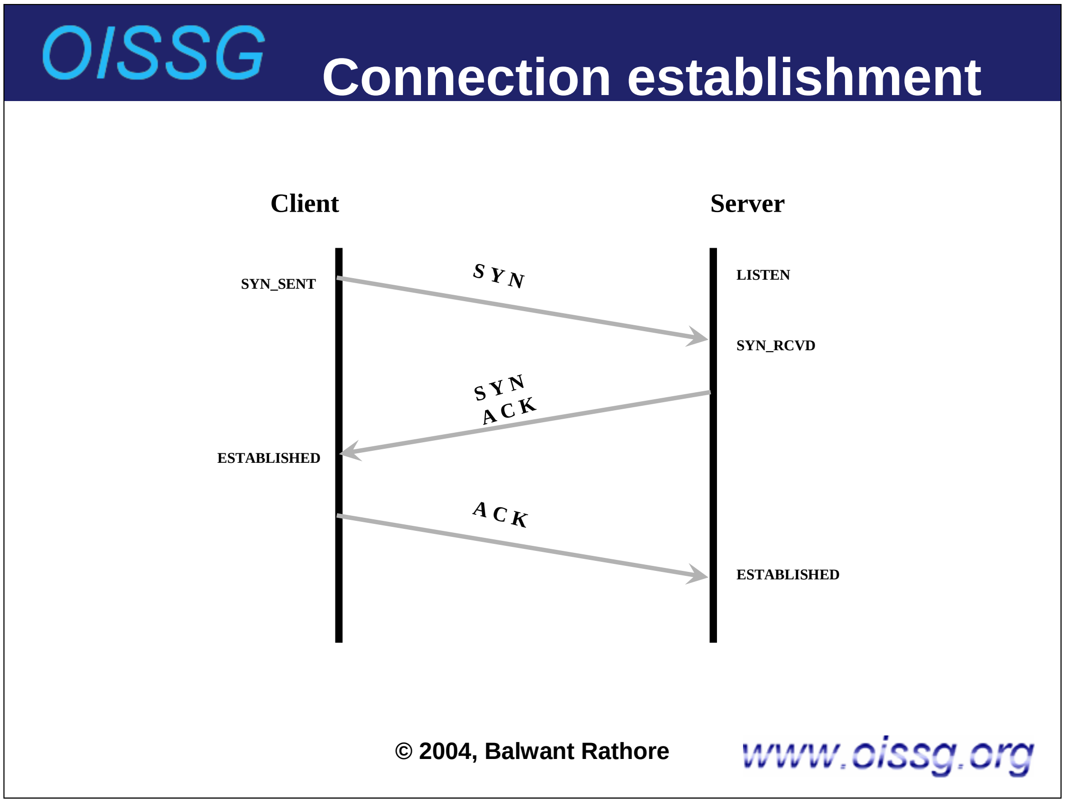
TCP states

- Connection termination
  - FIN_WAIT_1- Indicates active close
  - TIMED_WAIT– Client is in this state after active close
  - CLOSE_WAIT– Server just received FIN from client
  - LAST_ACK - Server just send its own FIN
  - CLOSED - Server received ACK from client

www.oissg.org

TCP states at the time of connection termination:

- FIN_WAIT_1- Indicates active close
- TIMED_WAIT– Client is in this state after active close
- CLOSE_WAIT– Server just received FIN from client
- LAST_ACK - Server just send its own FIN
- CLOSED - Server received ACK from client



OISSG

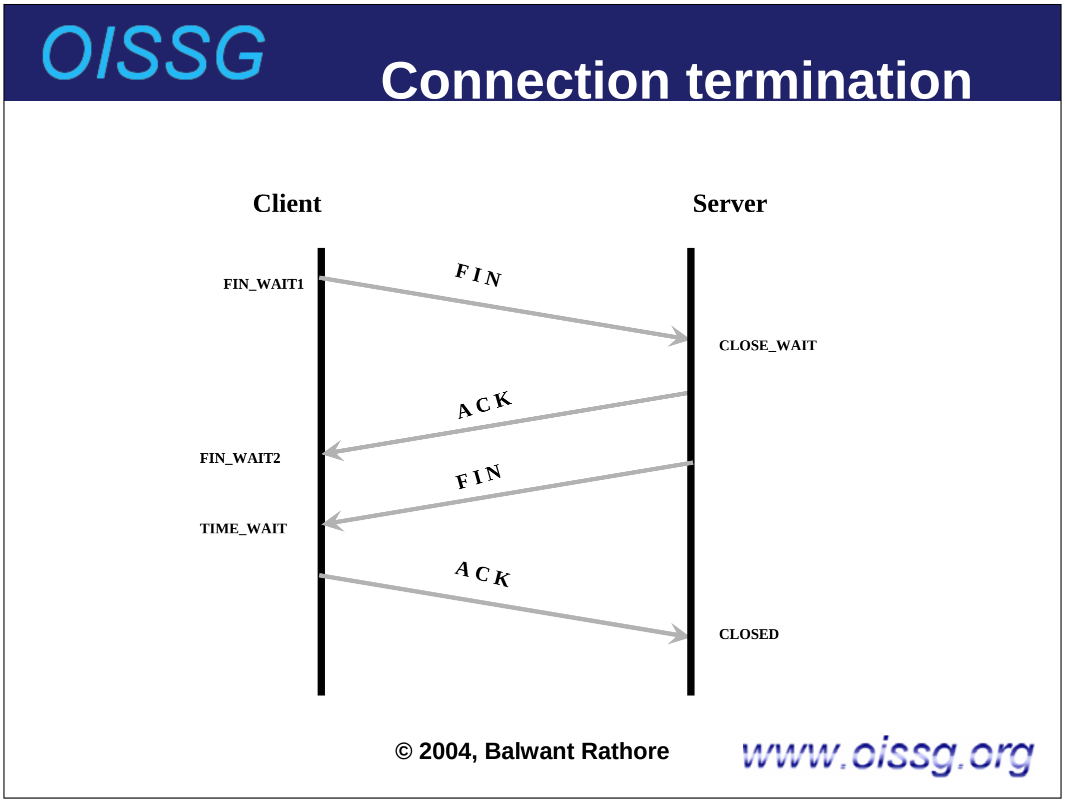
Connection establishment

© 2004, Balwant Rathore

www.oissg.org

First, source host sends a SYN packet to destination host, telling it the wish to establish a connection and setting its own ISN (Initial Sequence Number) in sequence number field. Upon receiving the request packet, the destination host sends back a SYN_ACK packet with its own ISN and the incremented ISN from source host. Finally, the source host will transmit an ACK packet and data transfer can take place.

There is one extra point need to mention. Suppose that host S did not send any SYN packet but received a SYN_ACK packet from host D, it would just send back a RST packet to reset the connection.



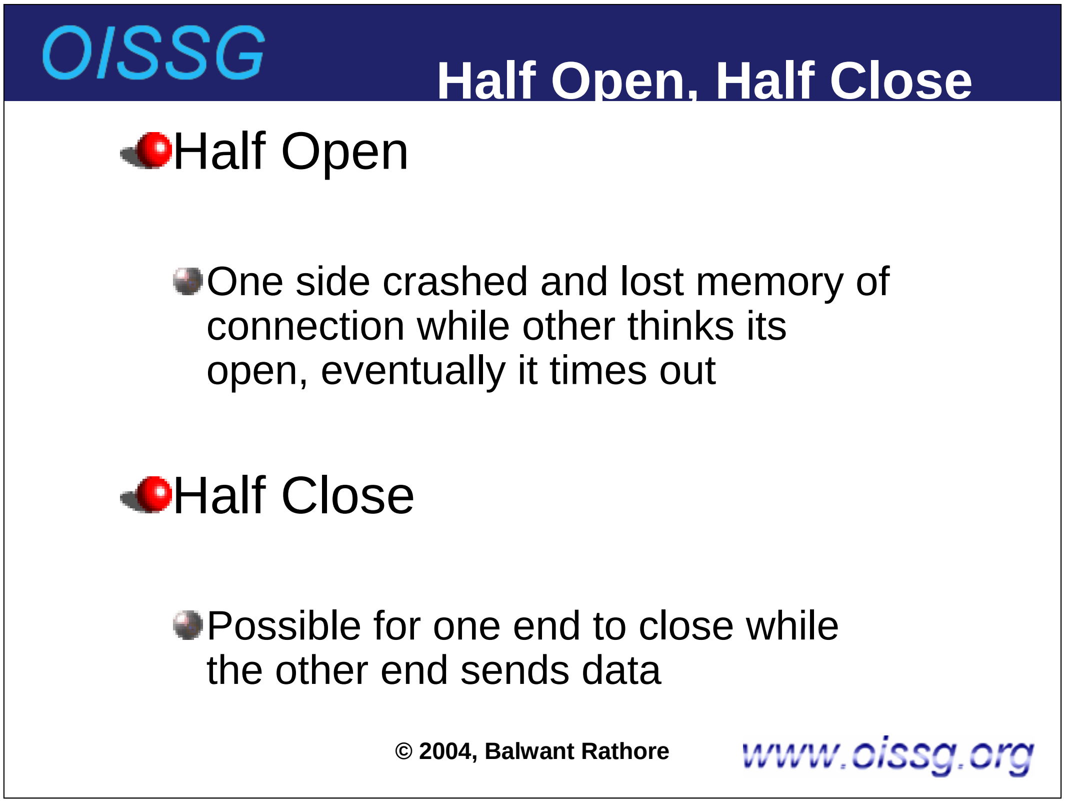
OISSG

Connection termination

© 2004, Balwant Rathore

www.oissg.org

First, source host sends a FIN packet to destination host, telling it to close the connection, the destination host sends back a SYN_ACK packet. Finally, the destination host sends FIN packet to the source host to terminate the connection. As soon as the source sends the ACK packet to the destination host the connection terminates.



OISSG

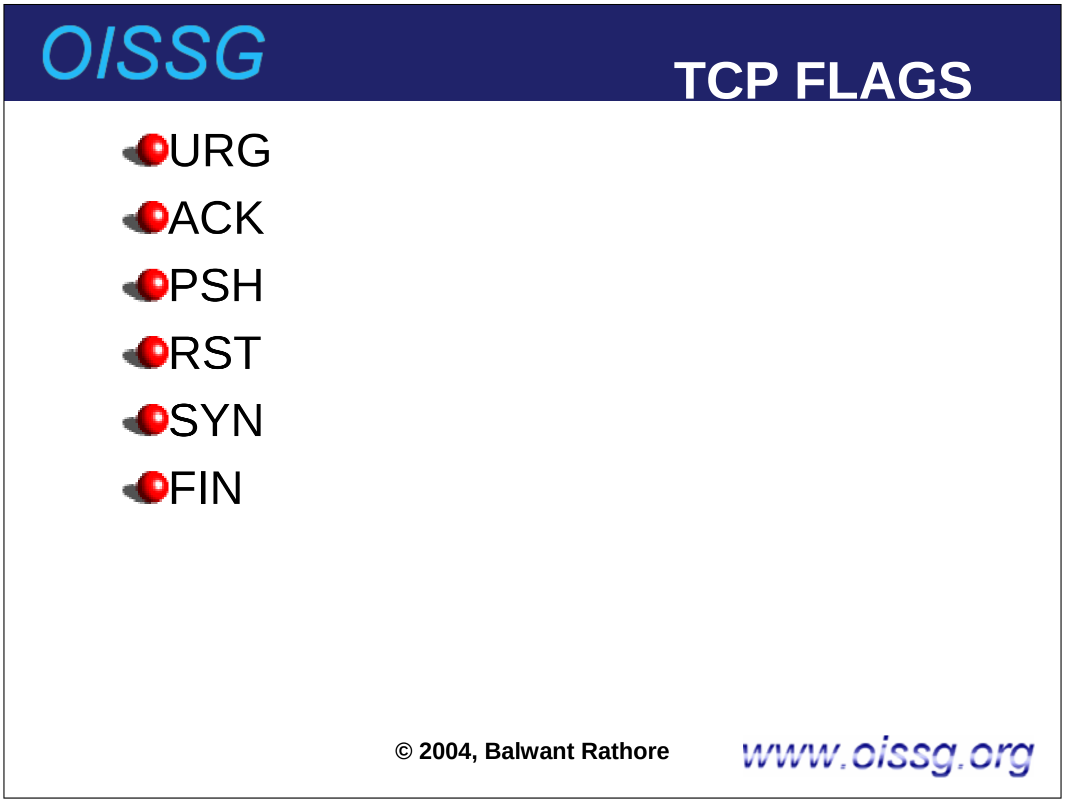
Half Open, Half Close

- Half Open
  - One side crashed and lost memory of connection while other thinks its open, eventually it times out
- Half Close
  - Possible for one end to close while the other end sends data

www.oissg.org

There is also problem of loss of connection like in :

- Half Open
- Full Open

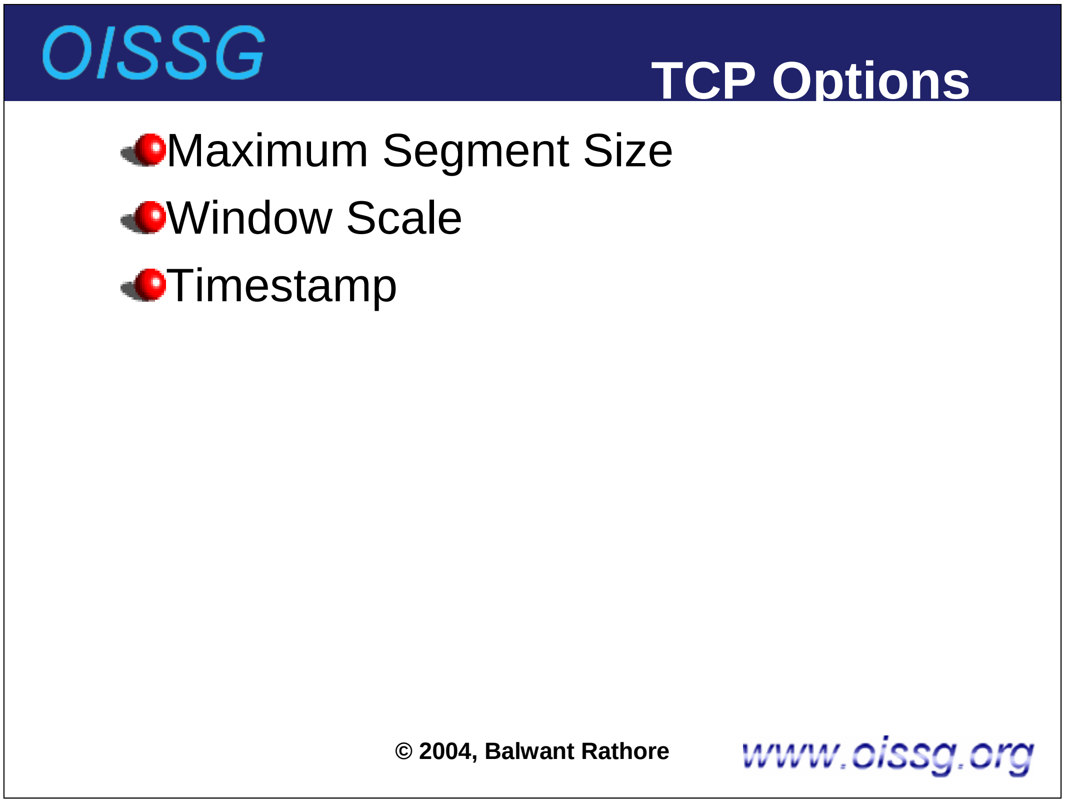


OISSG

TCP FLAGS

- URG
- ACK
- PSH
- RST
- SYN
- FIN

www.oissg.org



OISSG

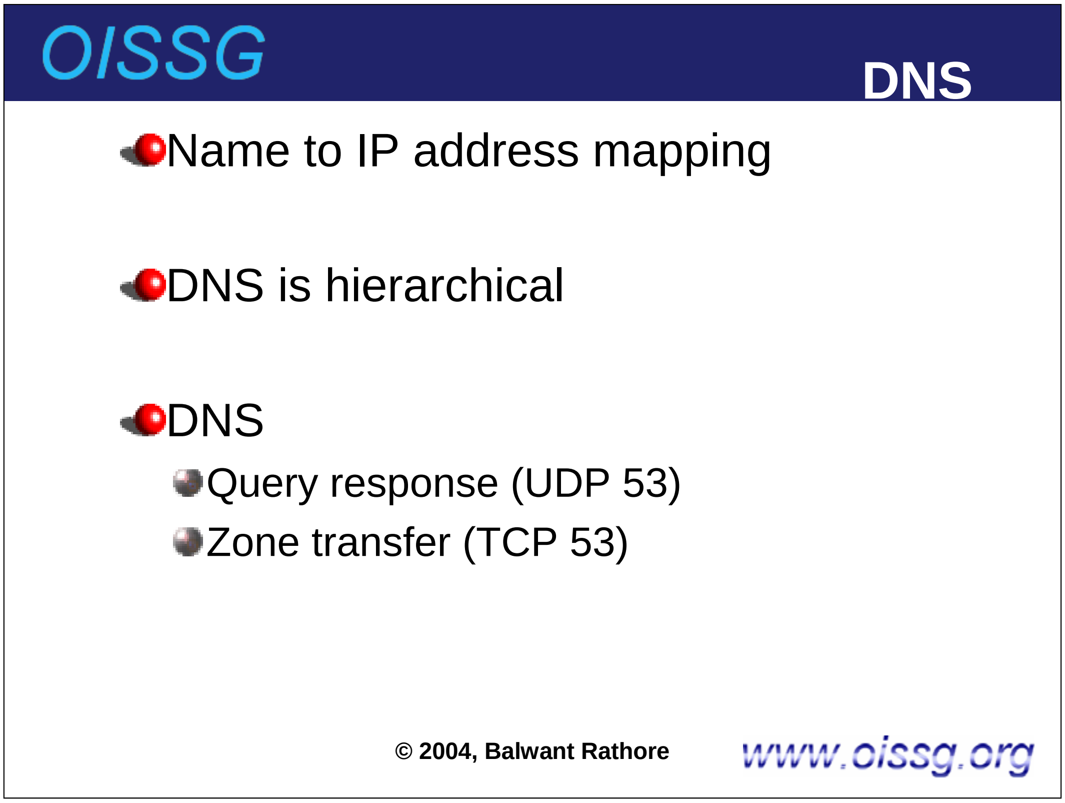
TCP Options

- Maximum Segment Size
- Window Scale
- Timestamp

© 2004, Balwant Rathore www.oissg.org

These are the options that can be used for TCP:

- Maximum Segment Size
- Window Scale
- Timestamp



OISSG

DNS

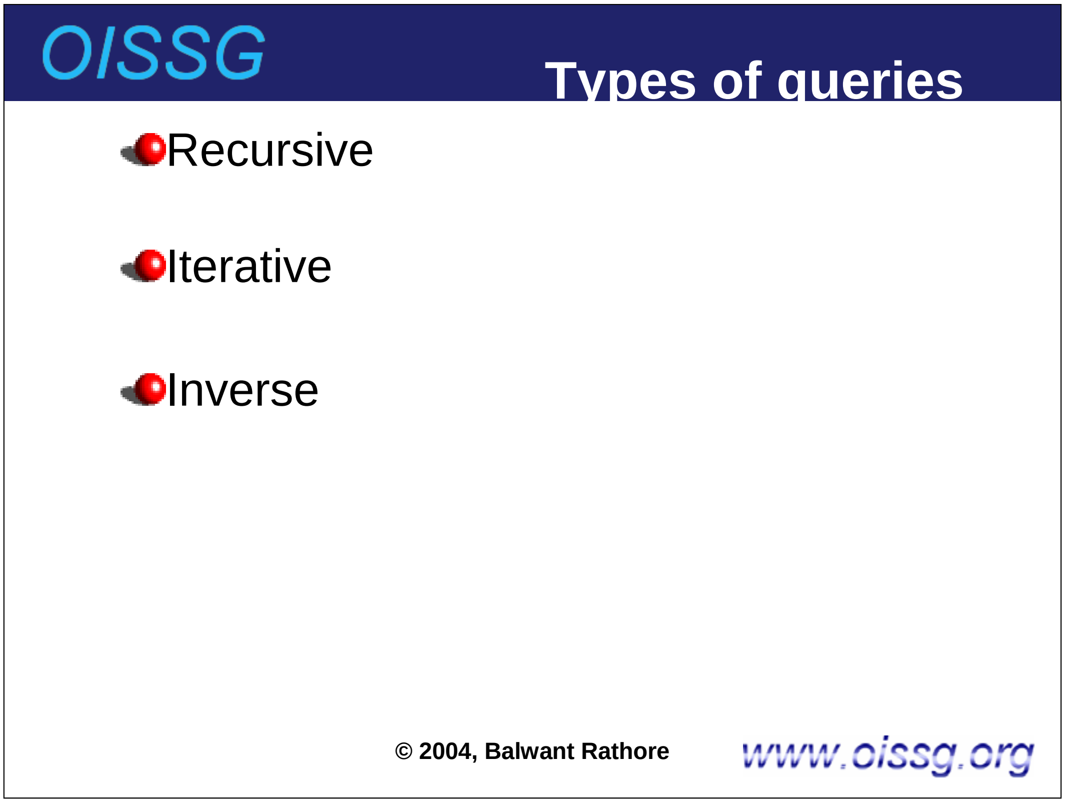
- Name to IP address mapping
- DNS is hierarchical
- DNS
  - Query response (UDP 53)
  - Zone transfer (TCP 53)

© 2004, Balwant Rathore

www.oissg.org

DNS is not inherent to TCP/IP protocol when it is first proposed. However, with millions of networks and hosts interconnected by the Internet, IP address becomes quite inconvenient for user level communications.

An alternative approach is to map low-level IP address into meaningful hostname, which is the main motivation of DNS. DNS is a distributed database system, which handles mapping high-level host names into low-level IP addresses, or vice versa. Much like routing infrastructures, DNS is composed by a large number of name servers in a distributed hierarchical architecture, while each individual name server handles requests from a limited domain. If a name server does not know how to resolve a particular query, it may forward the query to another name server, which either has much more information or is more specific to that particular domain which the query asked.



OISSG

Types of queries

- Recursive
- Iterative
- Inverse

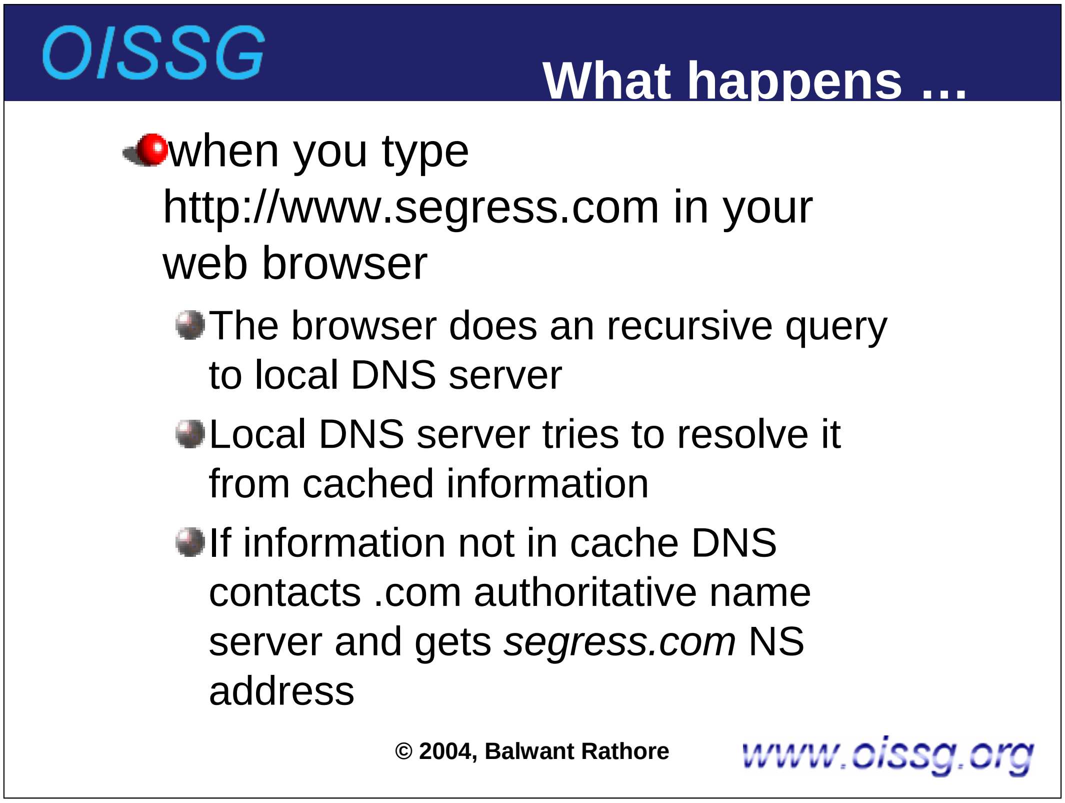
www.oissg.org

These are the types of queries

Recursive :- Host asks DNS server to give a complete answer to query

Iterative: - Host asks DNS server to give the best response without seeking assistance

Inverse: - To lookup an hostname given the IP Address



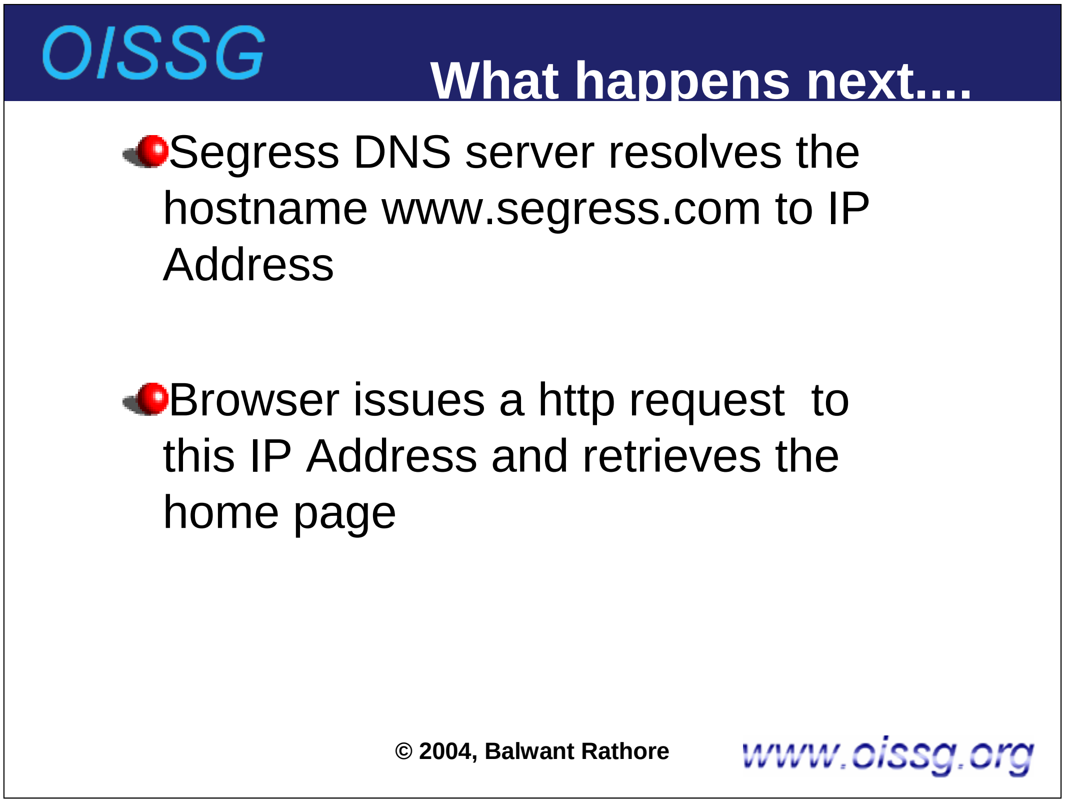
OISSG

What happens …

- when you type http://www.segress.com in your web browser
  - The browser does an recursive query to local DNS server
  - Local DNS server tries to resolve it from cached information
  - If information not in cache DNS contacts .com authoritative name server and gets *segress.com* NS address

www.oissg.org

The process that how the DNS server locates the information for URL. It resolves the hostname to the IP Address



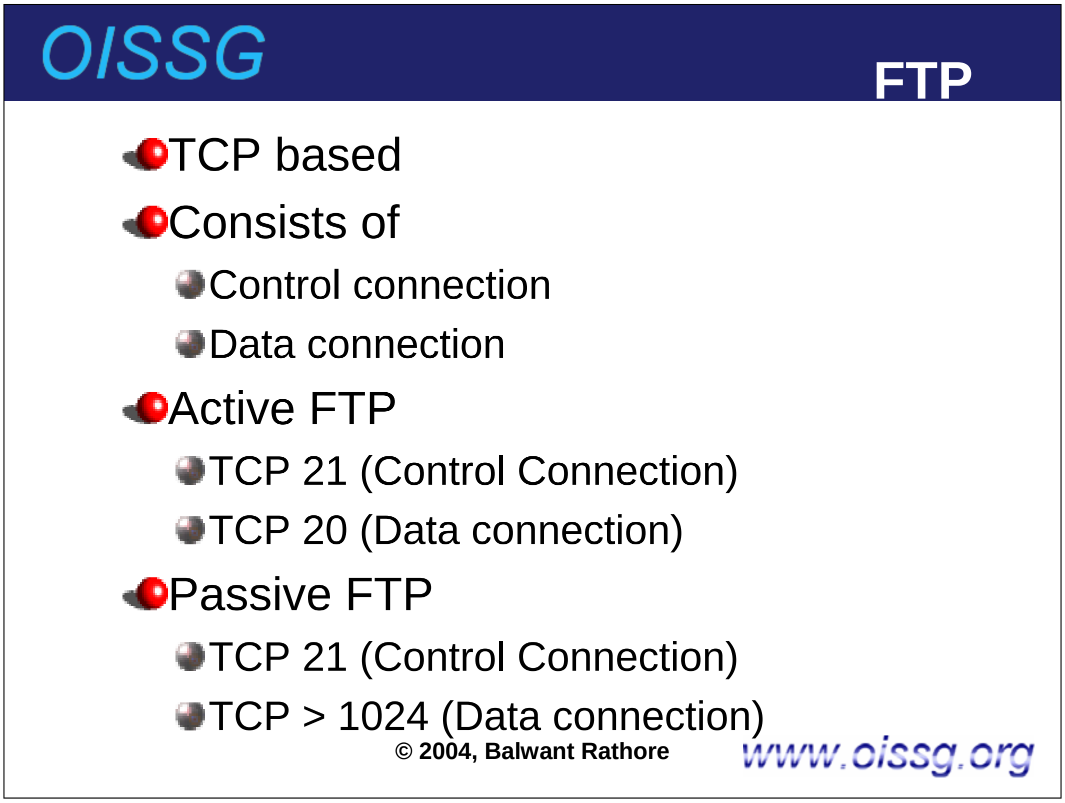
OISSG

What happens next....

- Segress DNS server resolves the hostname www.segress.com to IP Address
- Browser issues a http request to this IP Address and retrieves the home page

www.oissg.org

After resolving the IP Address from the host name, browser retrieves the homepage of the requested URL by issuing the HTTP request.



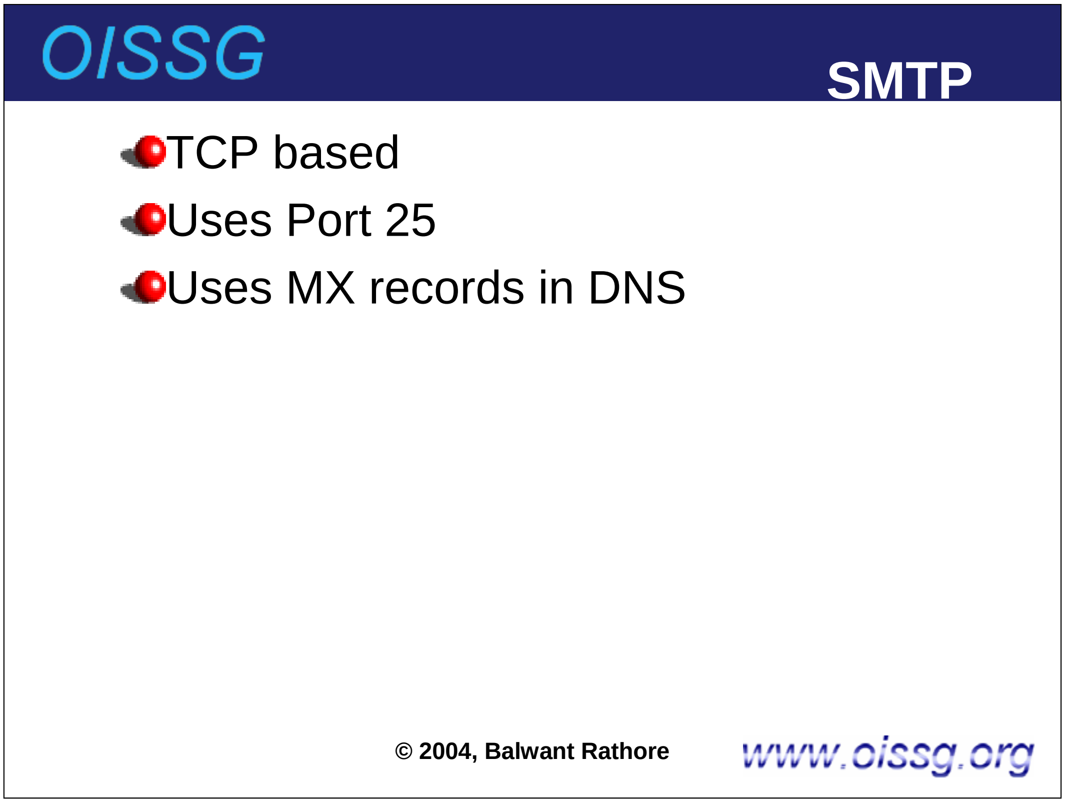
OISSG

FTP

- TCP based
- Consists of
  - Control connection
  - Data connection
- Active FTP
  - TCP 21 (Control Connection)
  - TCP 20 (Data connection)
- Passive FTP
  - TCP 21 (Control Connection)
  - TCP > 1024 (Data connection)

www.oissg.org

FTP is also a TCP based service which consists of control connection and the data connection. The FTP works in two modes. First is the Active FTP and the second one is the passive FTP.



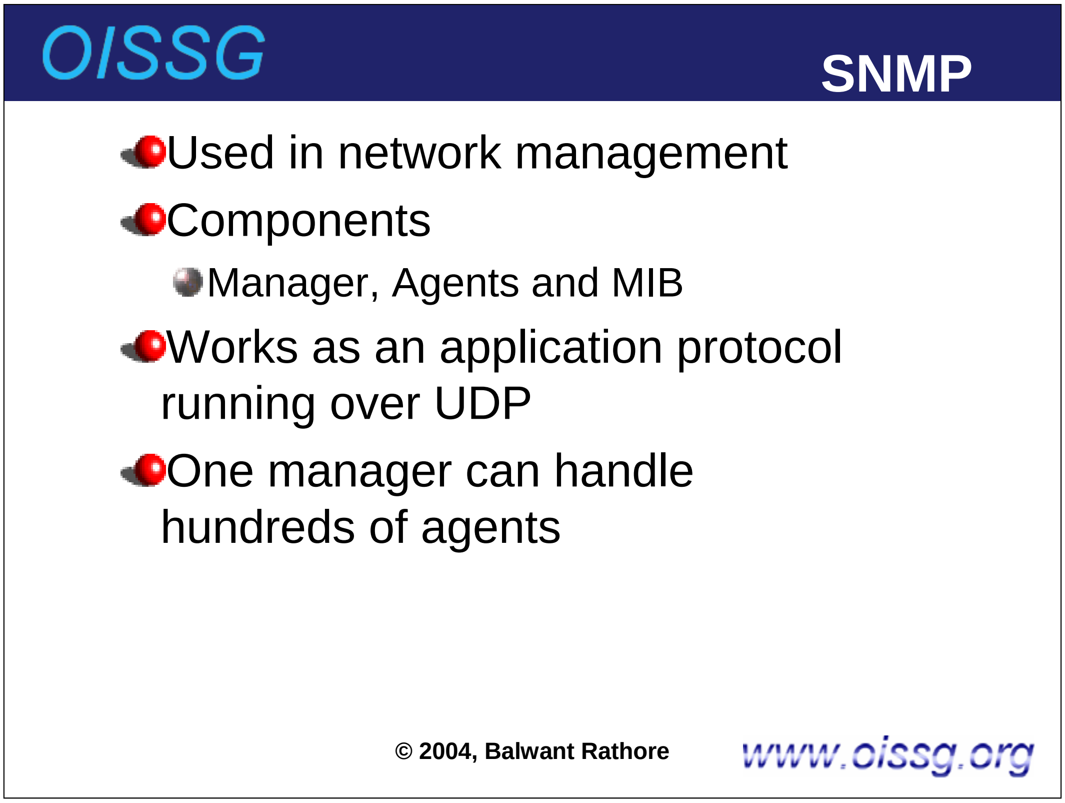
OISSG

SMTP

- TCP based
- Uses Port 25
- Uses MX records in DNS

www.oissg.org

It is a TCP based service that uses Port 25



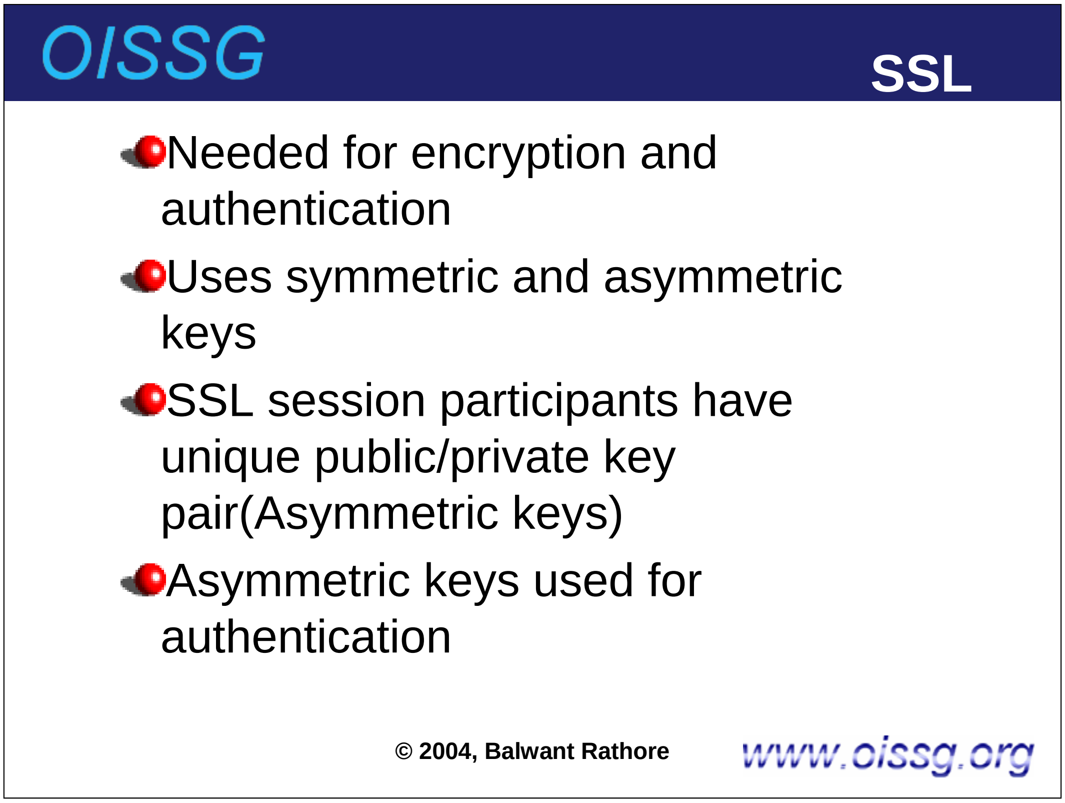
OISSG

SNMP

- Used in network management
- Components
  - Manager, Agents and MIB
- Works as an application protocol running over UDP
- One manager can handle hundreds of agents

www.oissg.org

A common method of router management is to use the Simple Network Management Protocol (SNMP). SNMP was not designed with authentication and data privacy features. It is recommended that SNMP is disabled on external routers, however if you must enable it, we recommend that a hard-to-guess community name is used and access is permitted only from specific hosts



OISSG

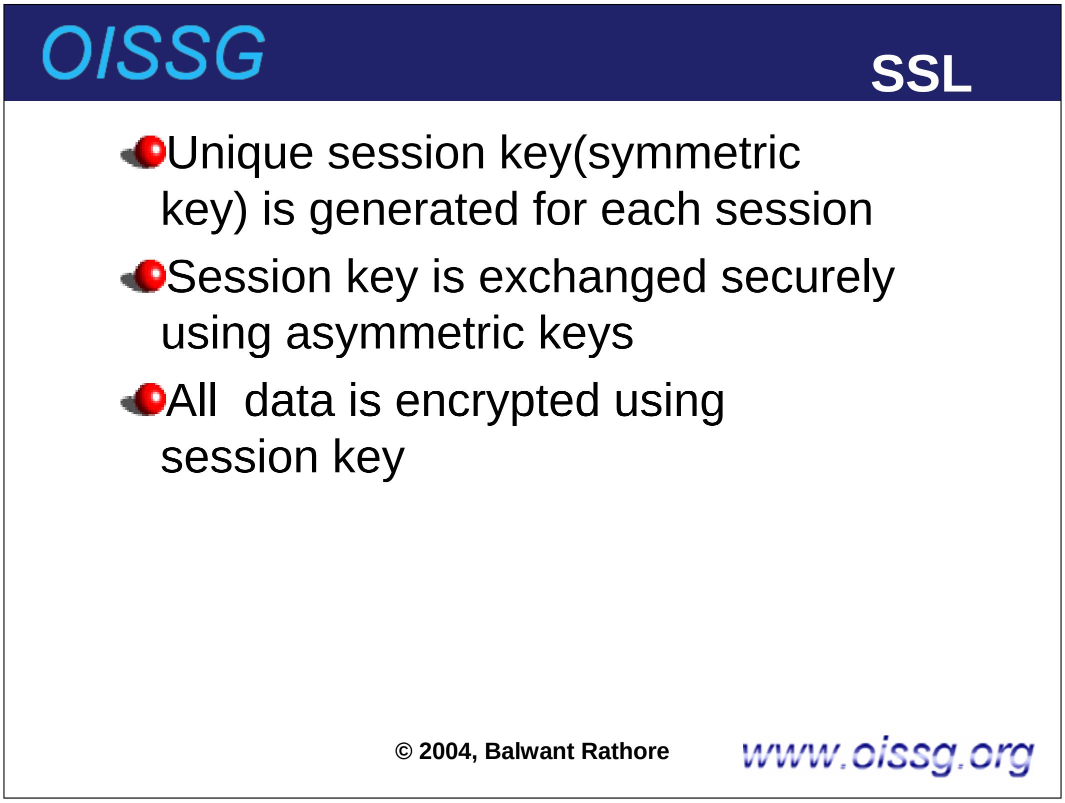
SSL

- Needed for encryption and authentication
- Uses symmetric and asymmetric keys
- SSL session participants have unique public/private key pair(Asymmetric keys)
- Asymmetric keys used for authentication

www.oissg.org

Secure Socket Layer: Very much important for security perspective.

A user that uses the Secure Socket Layer session must have the unique public/private key pair



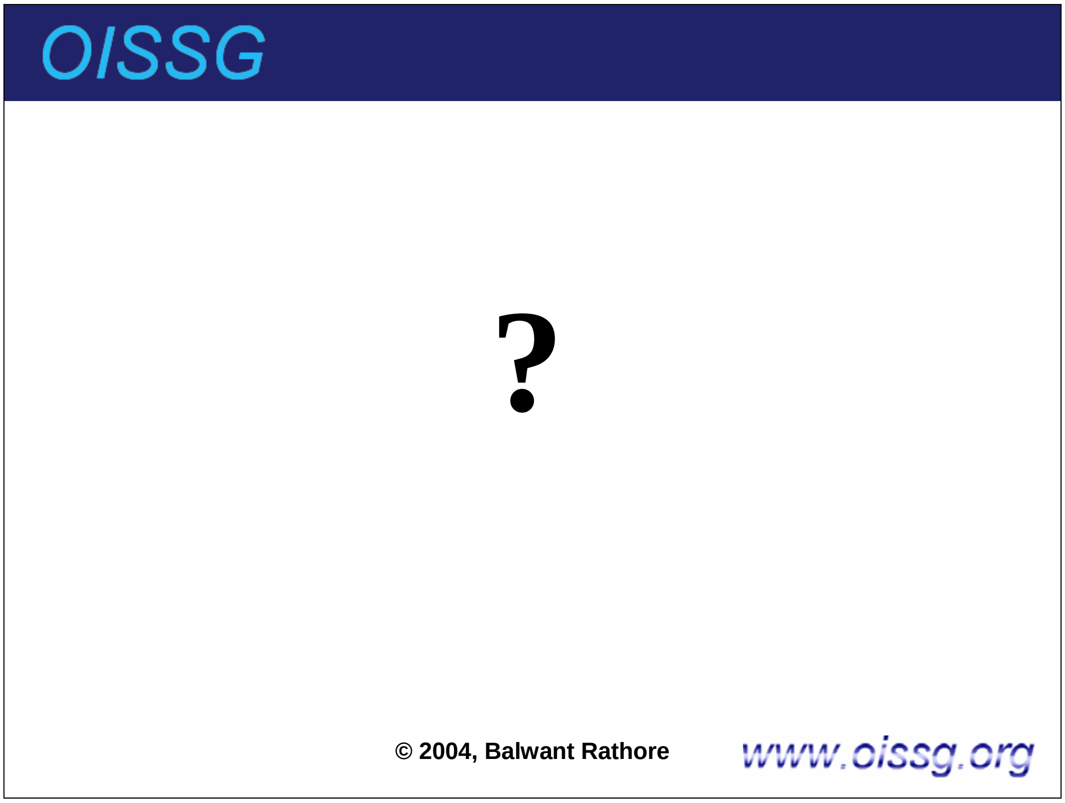
OISSG

SSL

- Unique session key(symmetric key) is generated for each session
- Session key is exchanged securely using asymmetric keys
- All data is encrypted using session key

www.oissg.org

The unique key is assigned to each and every session that are started and the session key (session ID) is exchanged securely using the asymmetric keys, making the session fairly session (no harm of stealing the session by anybody) and all the data is encrypted using the session keys.



OISSG

?

www.oissg.org

OISSG

Thanks for your time !

…

www.oissg.org