Network Layer (6): ICMP

Required reading:
Kurose 5.6

EECS 3214, Winter 2020
Instructor: N. Vlajic

1. Introduction
2. Router Architecture
3. Network Layer Protocols in the Internet
   - 4.1 IPv4
   - 4.2 IP Addressing and Subnetting
   - 4.3 ARP
   - **4.4 ICMP**
   - 4.5 IPv6
5. Routing Algorithms
6. Routing in the Internet

IP Protocol Deficiencies

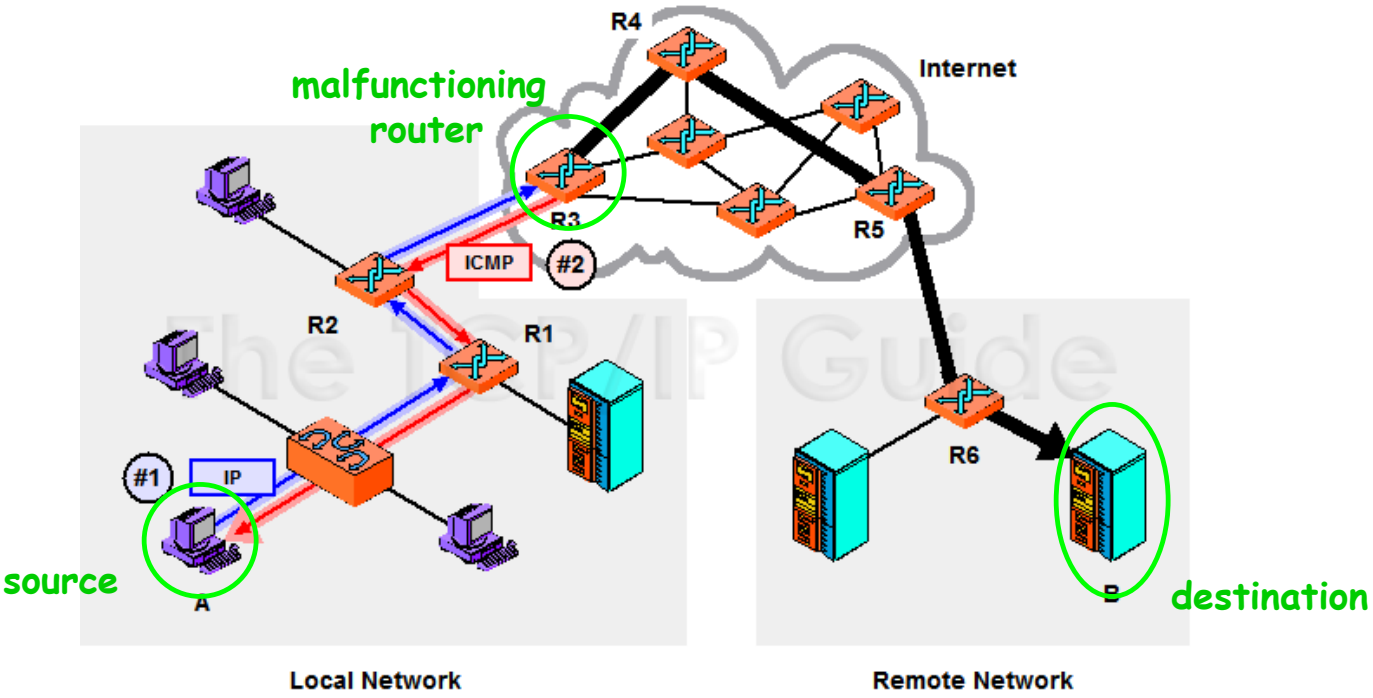
IP Deficiencies – **lack of error control** (i.e. error-reporting and error-correcting) **and network assistance mechanisms**

error handling

- what if a router must discard a datagram because the datagram's TTL = 0 ?!
- what if the final host must discard a number of fragments because it has not received all fragments by a certain time?!

diagnostics

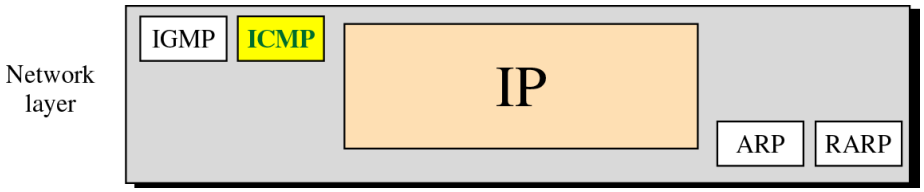
- what if a host needs to determine if another host/router is alive ?!

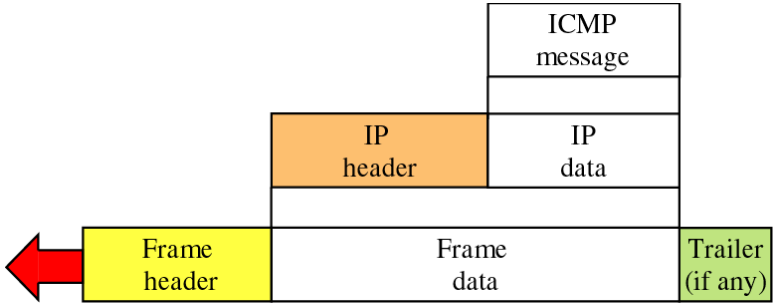


ICMP

ICMP – **Internet Control Message Protocol – 'companion' to IP, intended to compensate for IP deficiencies**

- **ICMP is network layer protocol "above IP" – its messages are not directly passed to data-link layer; they are first encapsulated inside IP datagrams**
- **IP header's "protocol field" set to 1 if the packet carries an ICMP message**



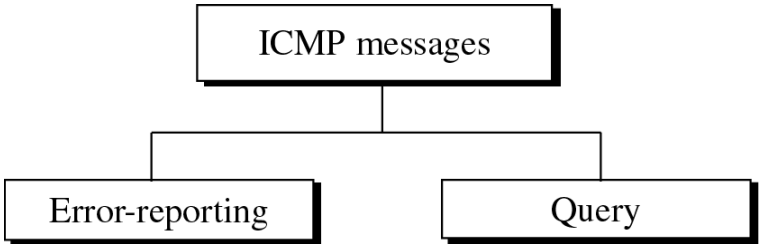


The ultimate destination of an ICMP message is not an application program or user on the destination machine, but the Internet Protocol software of that machine !

Types of ICMP Messages

ICMP Messages – **are divided into two broad categories:**

- **Error-reporting – report problems a router or a destination host may encounter when processing one specific IP packet**
- **Query – help a host or a network manager get specific info from a router or another host – occur in pairs request/reply**



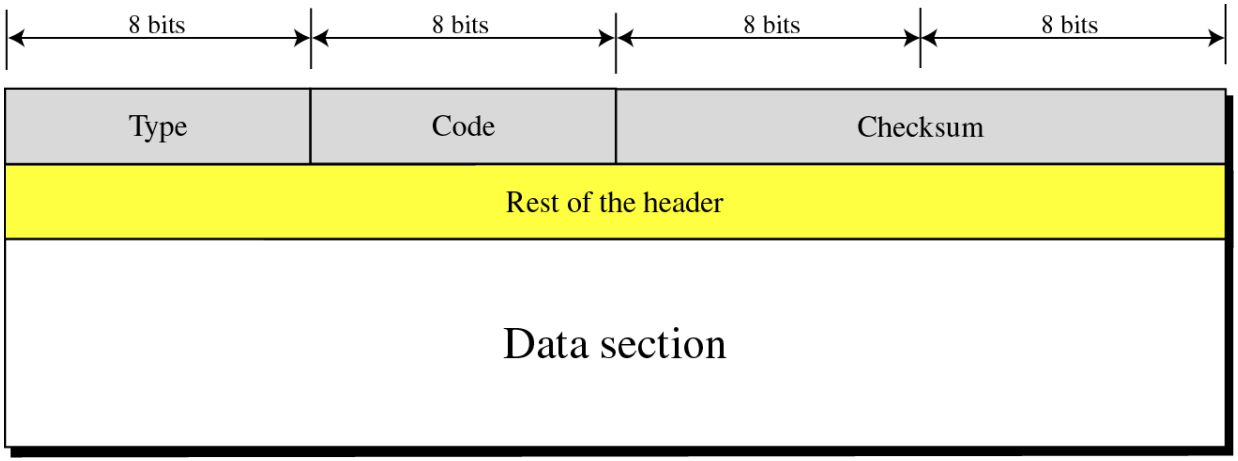
Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

From "TCP/IP Protocol Suite" by B. Forouzan, 4/e, pp. 246

ICMP Message Format

ICMP Message Format – **8 byte header + variable size data section**

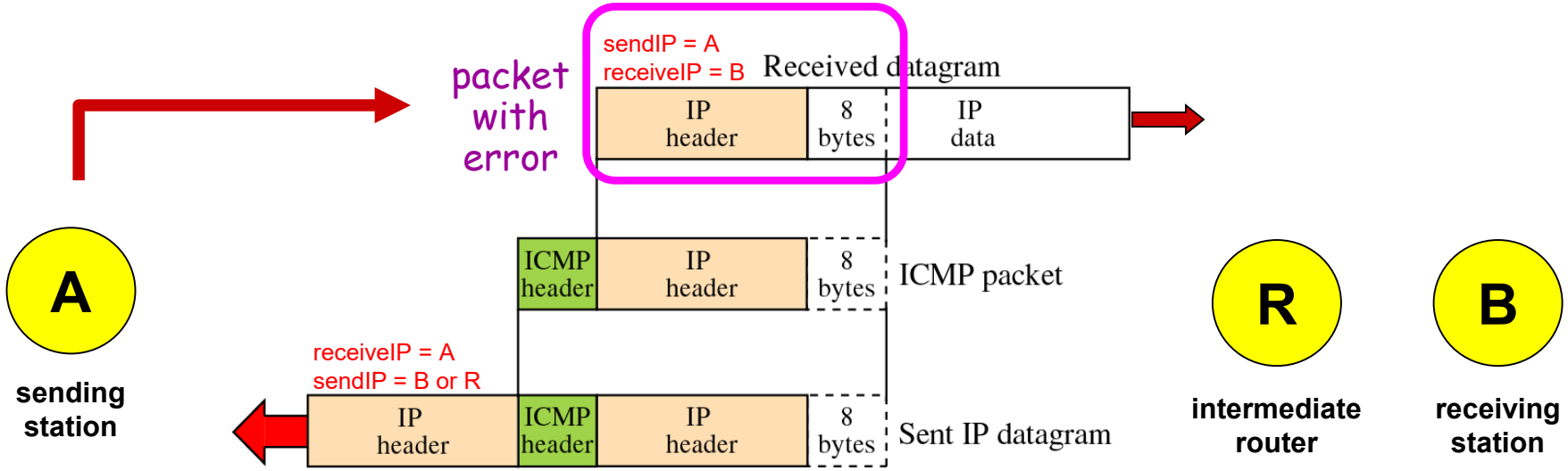
- first 4 bytes of header are the same for all message types, last 4 differ
- **type field in header** defines type of message
- **code field in header** specified reason for particular message type
- **checksum in header** is calculated over entire message
- **data in error messages** carries information for finding original packet that had error
- **data in query messages** carries extra information based on type of query



ICMP Error Reporting

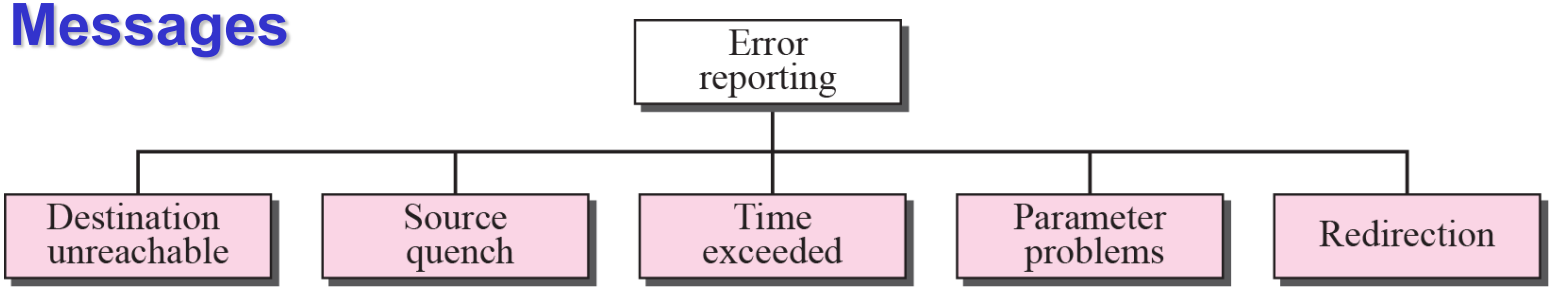
Error Reporting – **ICMP does not correct errors, it simply reports them – error correction is left to higher-level protocols**

- **error messages are always sent back to original source – only information available in datagram about route is source and destination IP address**
- **data section in all error messages contains IP header of original datagram + 8 bytes of data in that datagram**
  - **in case of UDP and TCP protocol first 8 bytes provide info about port and sequence number – this info is needed so that source can inform UDP and TCP about error**



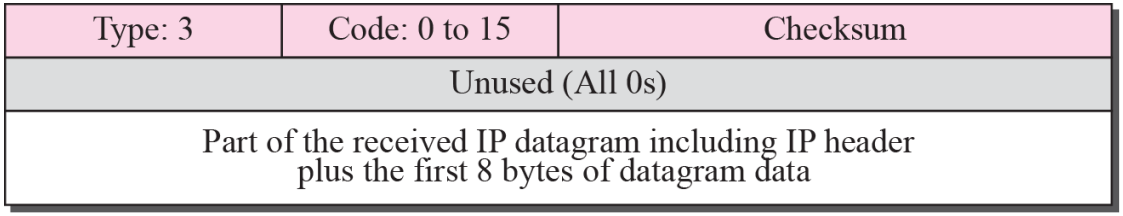
ICMP Error Reporting (cont.)

Error Reporting ICMP Messages



(1) Destination Unreachable – **when a router cannot route or host cannot deliver datagram, datagram is discarded and 'destination unreachable' message is sent back to source host**

	Implementation
Host	Mandatory.
Router	Mandatory.



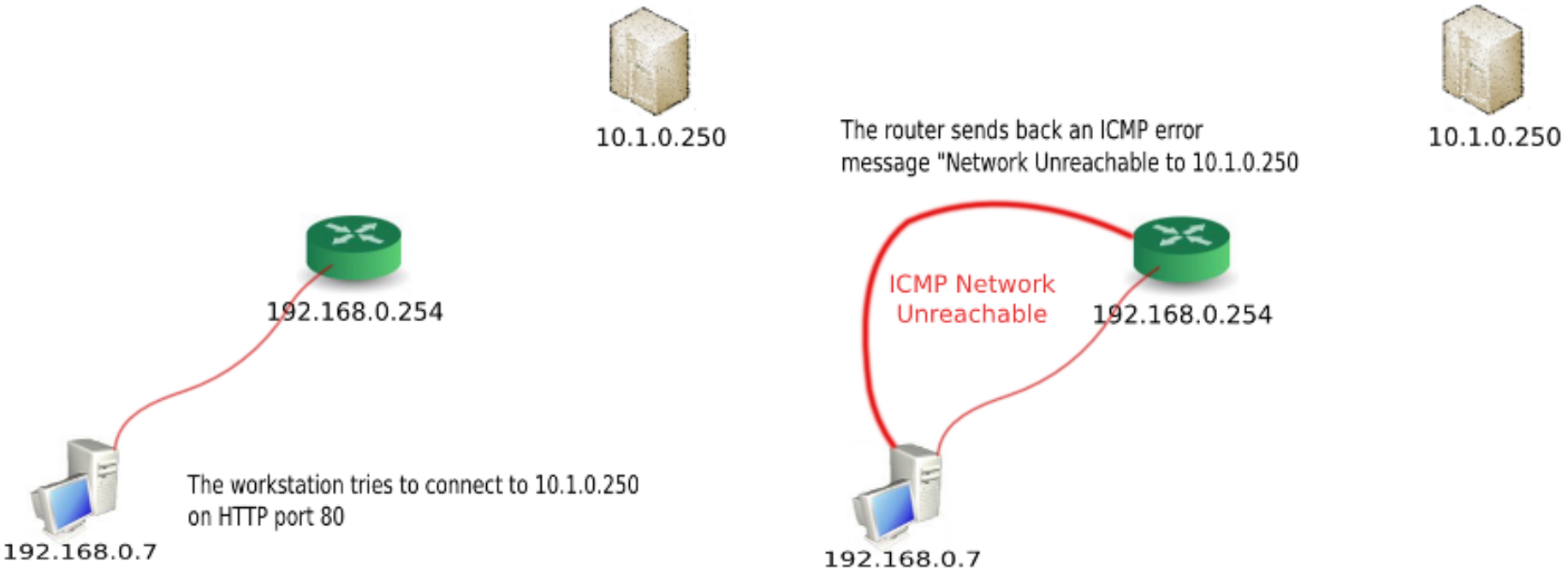
Code 0: destination network is unreachable – no current routes available
Code 1: destination host is unreachable, possibly due to hardware failure
Code 2: (destination host) protocol is unreachable, e.g. UDP or TCP protocol/module not running at the moment
Code 3: (destination host) port is unreachable – application program is not running at the moment
Code 7: destination host is unknown – the router is unaware of the destination host
Code 9: communication with the destination network is administratively prohibited
Code 10: communication with the destination host is administratively prohibited

ICMP Error Reporting (cont.)

Example [ICMP, Type 3, Code 0 – Destination Network Unreachable]

ICMP Network Unreachable

Let's take the simplest example: one machine sitting on a LAN (192.168.0.7), has one default gateway (192.168.0.254), which is the router. It is trying to reach a server, which does not sit on the LAN (10.1.0.250) and which cannot be reached, because 192.168.0.254 does not know how to route this traffic.



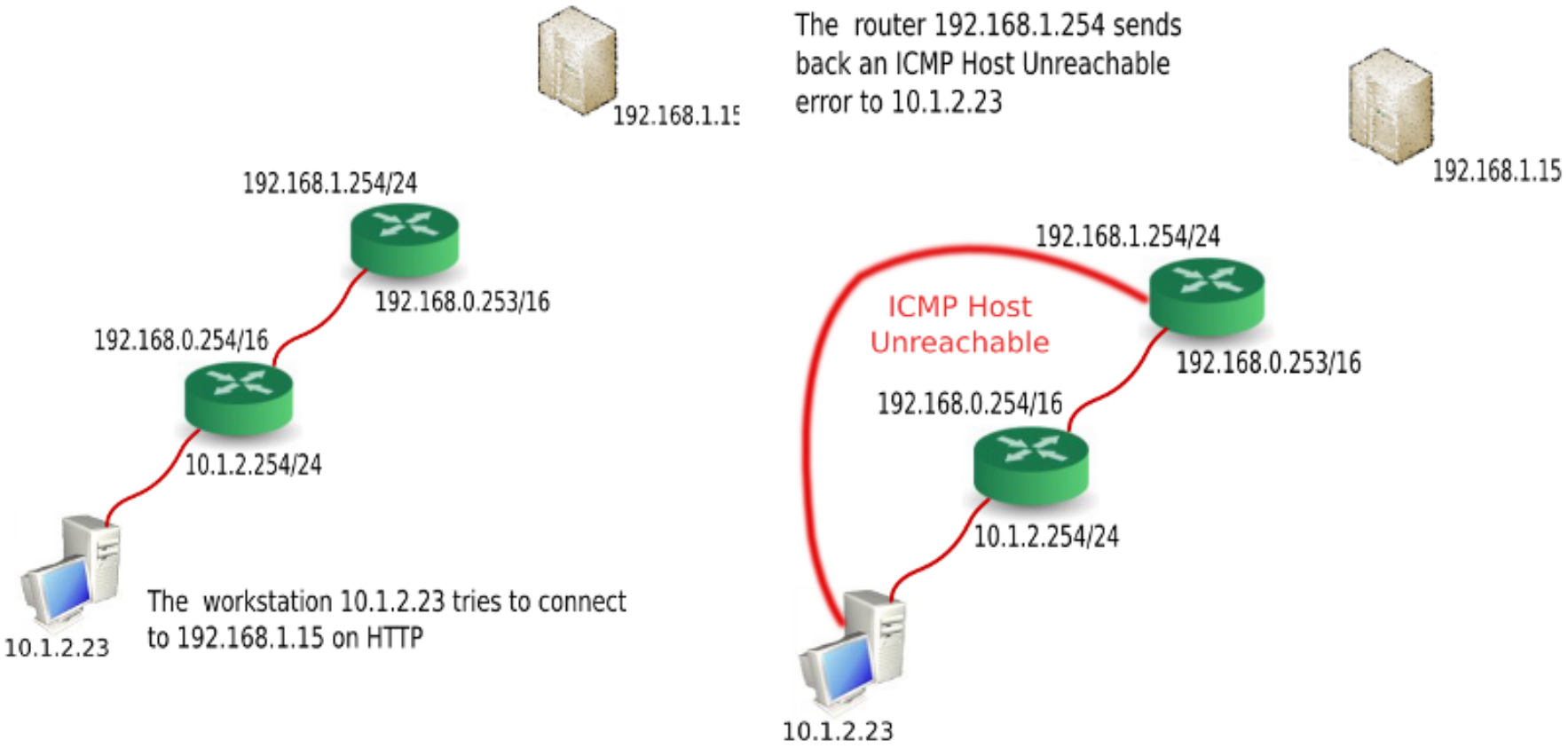
http://www.securactive.net/help/userguide/nova/last/html/interpreting_the_results.html

ICMP Error Reporting (cont.)

Example [ICMP, Type 3, Code 1 – Destination Host Unreachable]

ICMP Host Unreachable

Let's take the simplest example: one machine sitting on a LAN (10.1.2.23), has one default gateway (10.1.2.254/24), which is the router. It is trying to reach a server, which does not sit on the LAN (192.168.1.15). The traffic flows and reaches the last router before the server (192.168.1.254/24); this router cannot reach 192.168.1.15 (because it is unplugged, down or it does not exist).



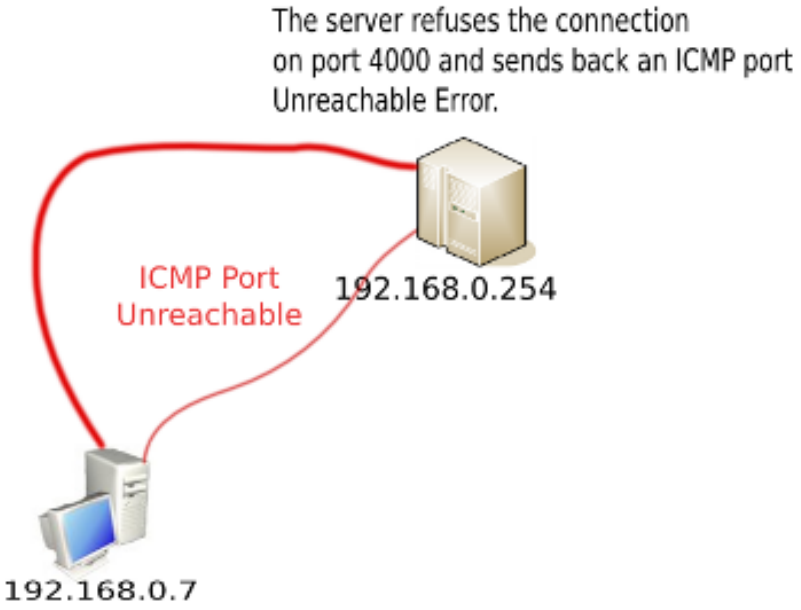
http://www.securactive.net/help/userguide/nova/last/html/interpreting_the_results.html

ICMP Error Reporting (cont.)

Example [ICMP, Type 3, Code 3 – Destination Port Unreachable]

ICMP Port Unreachable

Let's take a second example: one machine sitting on a LAN (192.168.0.7). It is trying to reach a server 192.168.0.254, which sits on the LAN on port UDP 4000, on which the server does not respond.



http://www.securactive.net/help/userguide/nova/last/html/interpreting_the_results.html

ICMP Error Reporting (cont.)

(2) Source Quench – **when a router / host a discards datagram due to congestion it sends 'source-quench' message to sender of datagram in order to**

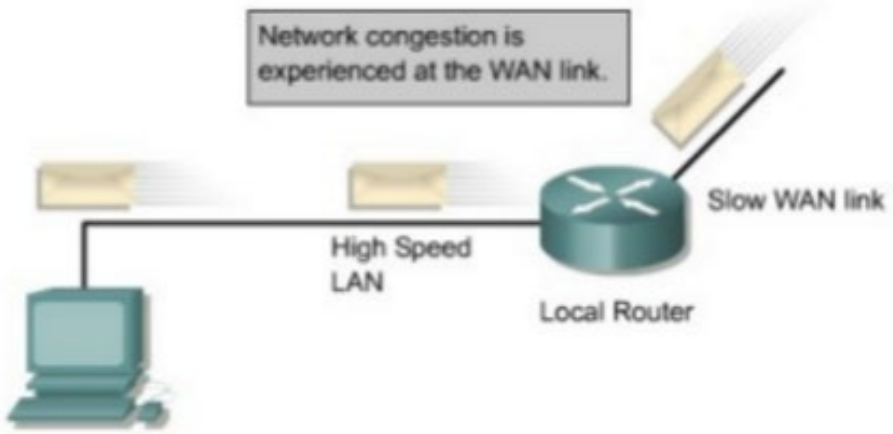
why optional?!

(a) inform source that datagram has been discarded

(b) warn source that there is congestion somewhere in the path – source should slow down (unreliable flow control!)

	Implementation
Host	Optional.
Router	Optional.

Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		



ICMP has no mechanism to tell the course that congestion has been relieved!

ICMP Error Reporting (cont.)

(3) Time Exceeded

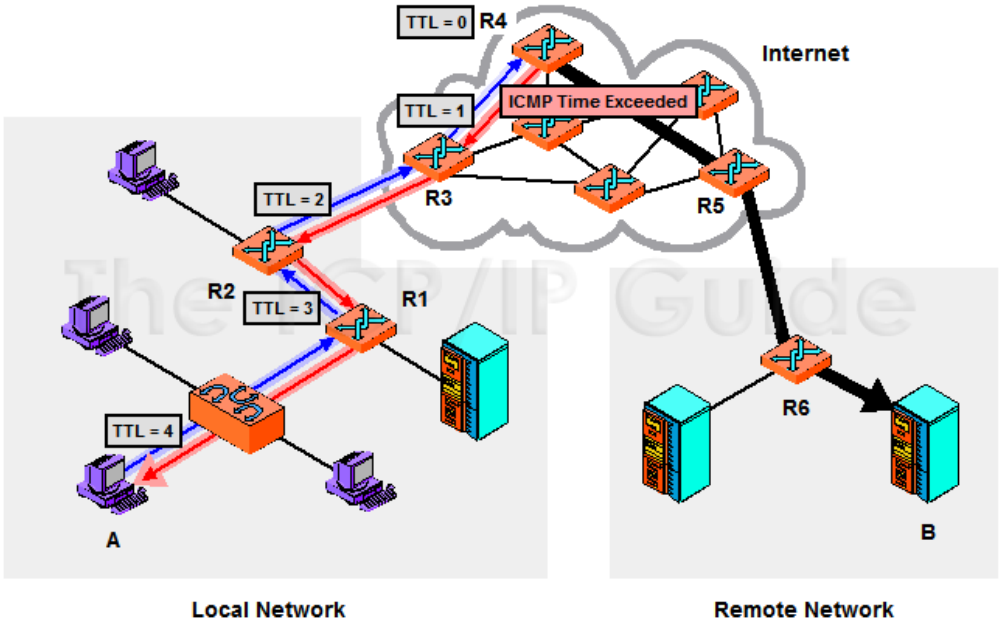
(a) whenever router decrements TTL to 0 in a datagram, it discards the datagram and sends 'time-exceeded' message (Code=0)

(b) when final destination does not receive all fragments in certain time interval it discards received fragments and sends 'time-exceeded' message to original source (Code=1)

	Implementation
Host	Optional.
Router	**Mandatory.**

Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

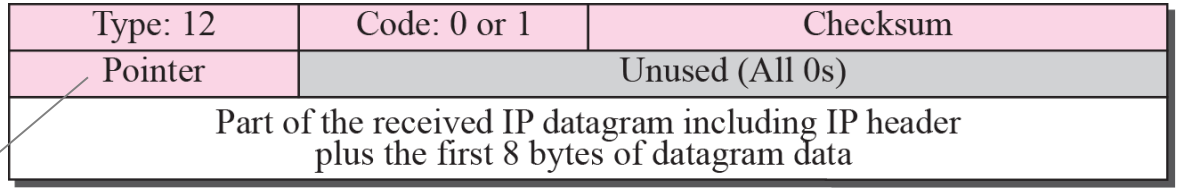
A sends a packet to B with TTL = 5



ICMP Error Reporting (cont.)

(4) Parameter Problem – if router / host discovers problematic or missing value in any field of the datagram it discards datagram and sends 'parameter problem' message back to source

	Implementation
Host	Mandatory.
Router	Mandatory.



Points to octet that caused problem.
Code 0 – problem in header
Code 1 – options field(s) is missing.

(5) Redirection – host usually starts with a small routing table that is gradually updated - one tool to accomplish this is 'redirection' message

(a) when host comes up its routing table has limited number of entries

(b) for this reason, host may send datagram to wrong router

(c) router that receives datagram will forward it to correct router

(d) to update host's routing table, router sends 'redirection' message to host

NOTE: although the redirection messages is considered an 'error reporting' messages, it is different form from other error messages – it does not discard the datagram; it sends it to appropriate router!

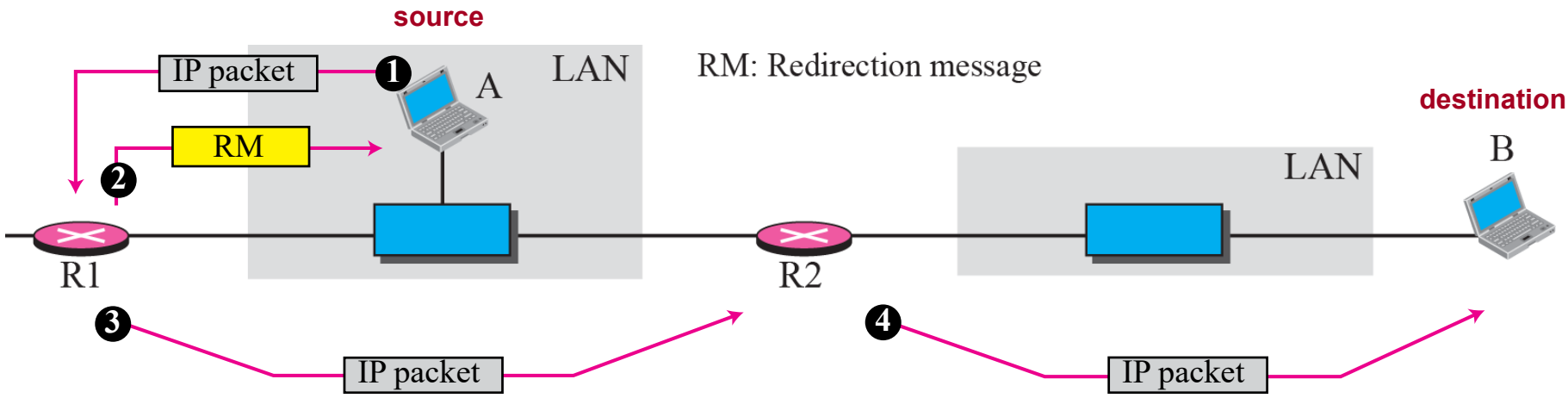
ICMP Error Reporting (cont.)

(5) Redirection (cont.)

	Implementation
Host	
Router	Mandatory.

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Code 0: **redirect for network error** – redirect all future datagrams sent to this network
Code 1: **redirect for host error** – redirect all future datagrams sent only to this specific device
Code 2: **redirect for TOS and network error** – Code 0 AND future datagrams with this ToS value
Code 3: **redirect for TOS and host error** – Code 1 AND future datagrams with this ToS value



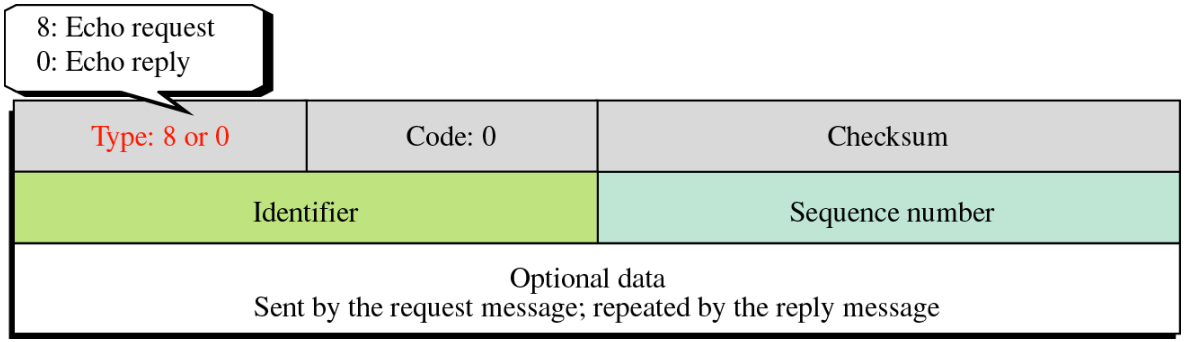
ICMP Query

Query Messages

(1) Echo Request and Reply – used for diagnostic purposes – two messages in combination determine whether two systems (host or routers) can communicate with each other

- node to be tested is sent an 'echo request'; optional data field contains a message that must be repeated exactly by responding node in 'echo-reply' message
- identifier and sequence number fields are not formally defined and can be used arbitrarily by the sender
- echo request and echo reply are used by ping when checking if another host is reachable

	Implementation
Host	Mandatory.
Router	Mandatory.



ICMP Query (cont.)

(2) Timestamp Request and Reply

– used to determine transmission vs. processing component of RTT between two hosts or routers

- original timestamp is filled by source at 'timestamp request' departure time
- receive timestamp is filled by destination at the time 'timestamp request' was received
- transmit timestamp is filled by destination at the time 'timestamp reply' departs
- roundtrip calculations are correct even if two clocks are not synchronized – each clock contributes 2x to calculation

Sending time = value of receive timestamp - value of original timestamp
Receiving time = time the packet returned - value of transmit timestamp
RTT = sending time + receiving time

	Implementation
Host	Optional.
Router	Optional.