إدارة الشبكات الحاسوبية

د.م. علي ذياب

بروتوكولات إدارة الشبكة (Network Management Protocols)

محتويات المحاضرة

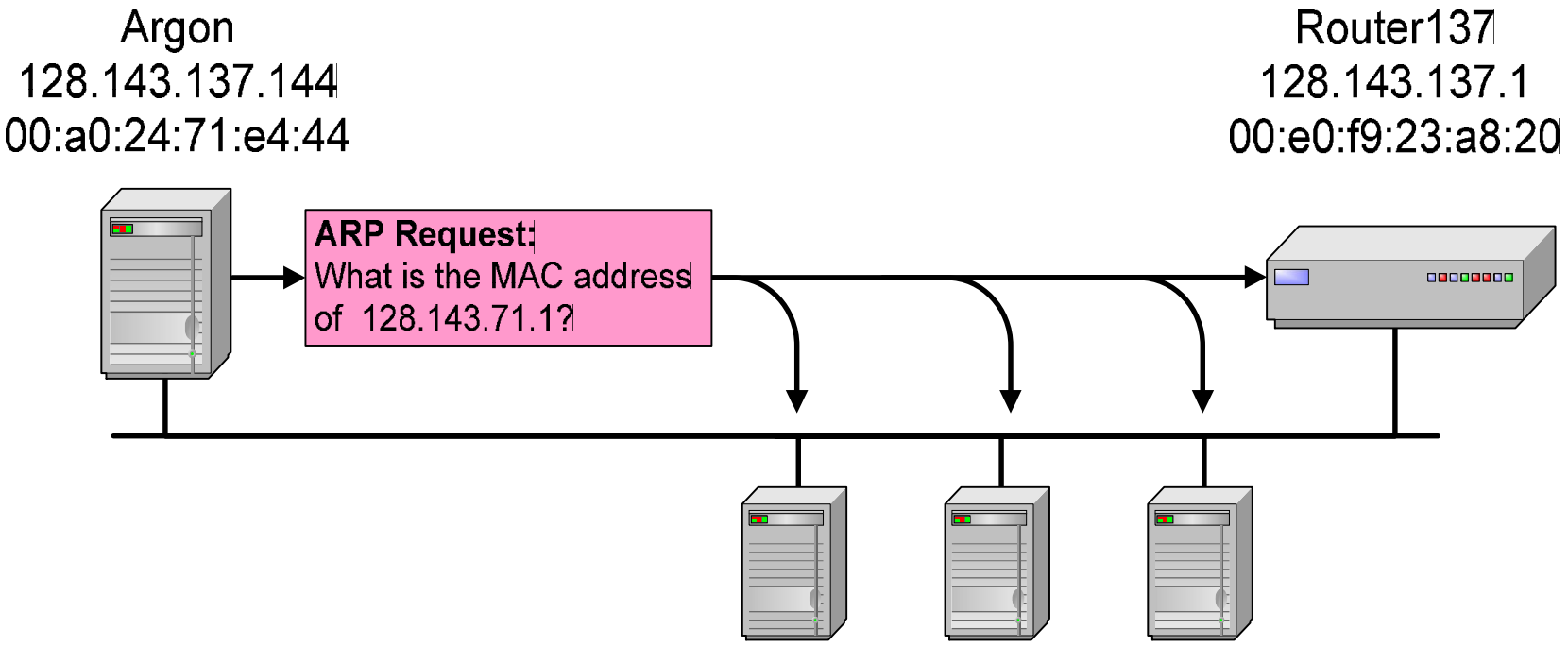
- بروتوكول الإعداد الديناميكي للمضيف (Dynamic Host Configuration Protocol (DHCP)
- IntServ
- RSVP
- بروتوكولات إدارة البريد الإلكتروني (eMail Management Protocols)
- النفاذ عن بعد (Remote access)

بروتوكول الإعداد الديناميكي للمضيف (Dynamic Host Configuration Protocol (DHCP)

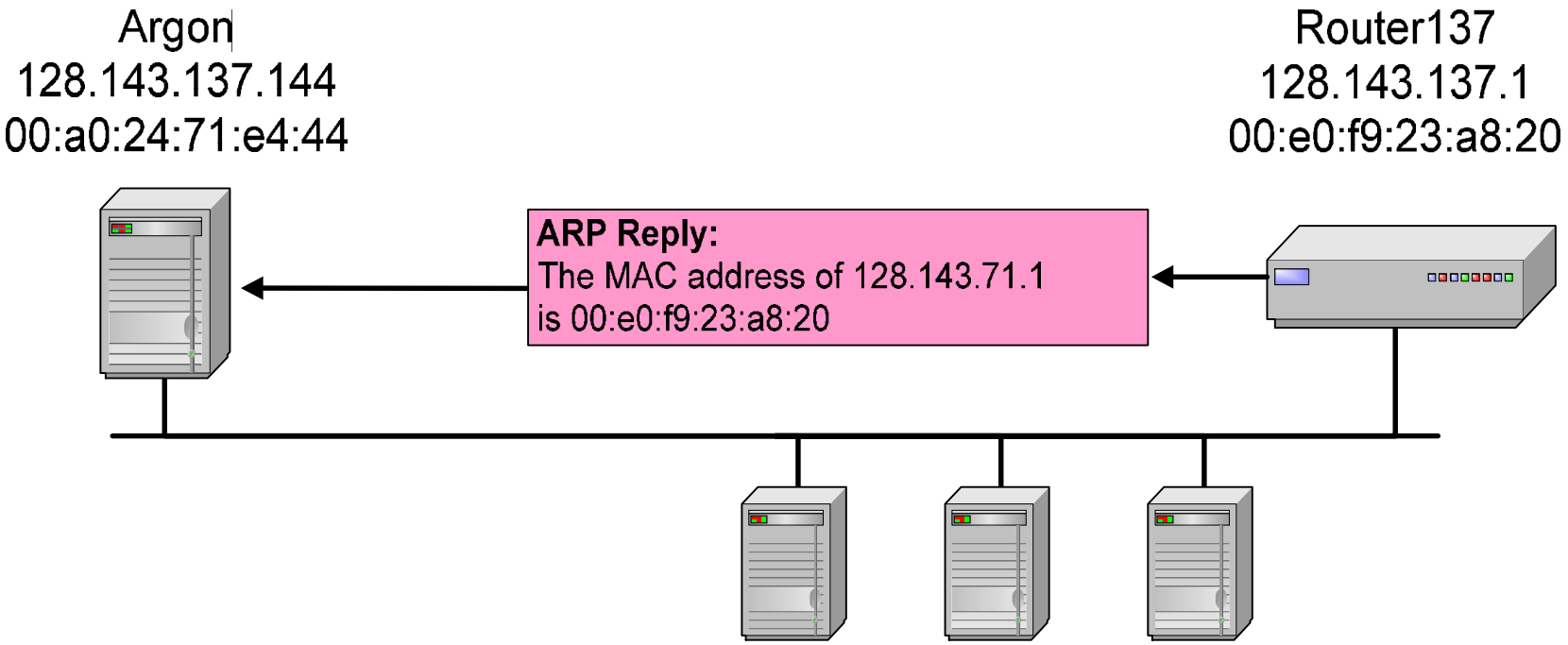
حلول أخرى للتخصيص الديناميكي للعناوين

- Reverse Address Resolution Protocol (RARP)
  - يعمل بشكل مشابه لـ ARP
  - يقوم بإعادة عنوان IP لعنوان MAC معين
  - تمّ استبداله بـ BOOTP و لاحقاً بـ DHCP
  - استُخدم من أجل اللأجهزة التي لم تكن تمتلك قرص تخزين, كمثل الطرفيات الموصولة لمخدم.
- سنستعرض فيما يلي آلية عمل بروتوكولي ARP و RARP

حلول أخرى للتخصيص الديناميكي للعناوين

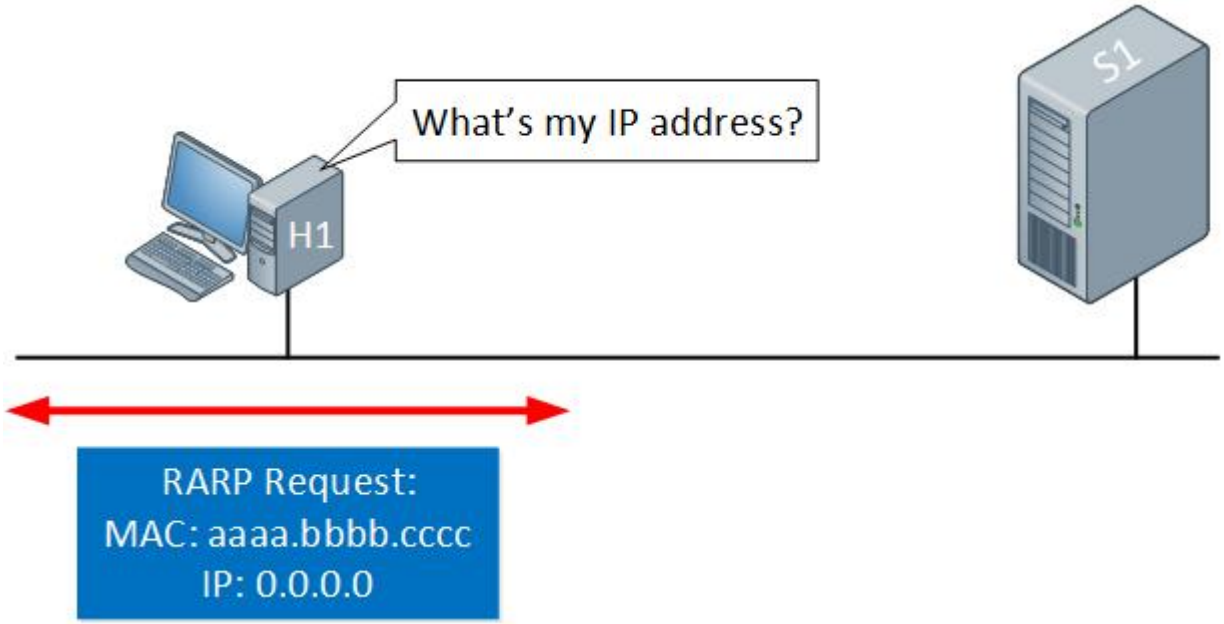


حلول أخرى للتخصيص الديناميكي للعناوين

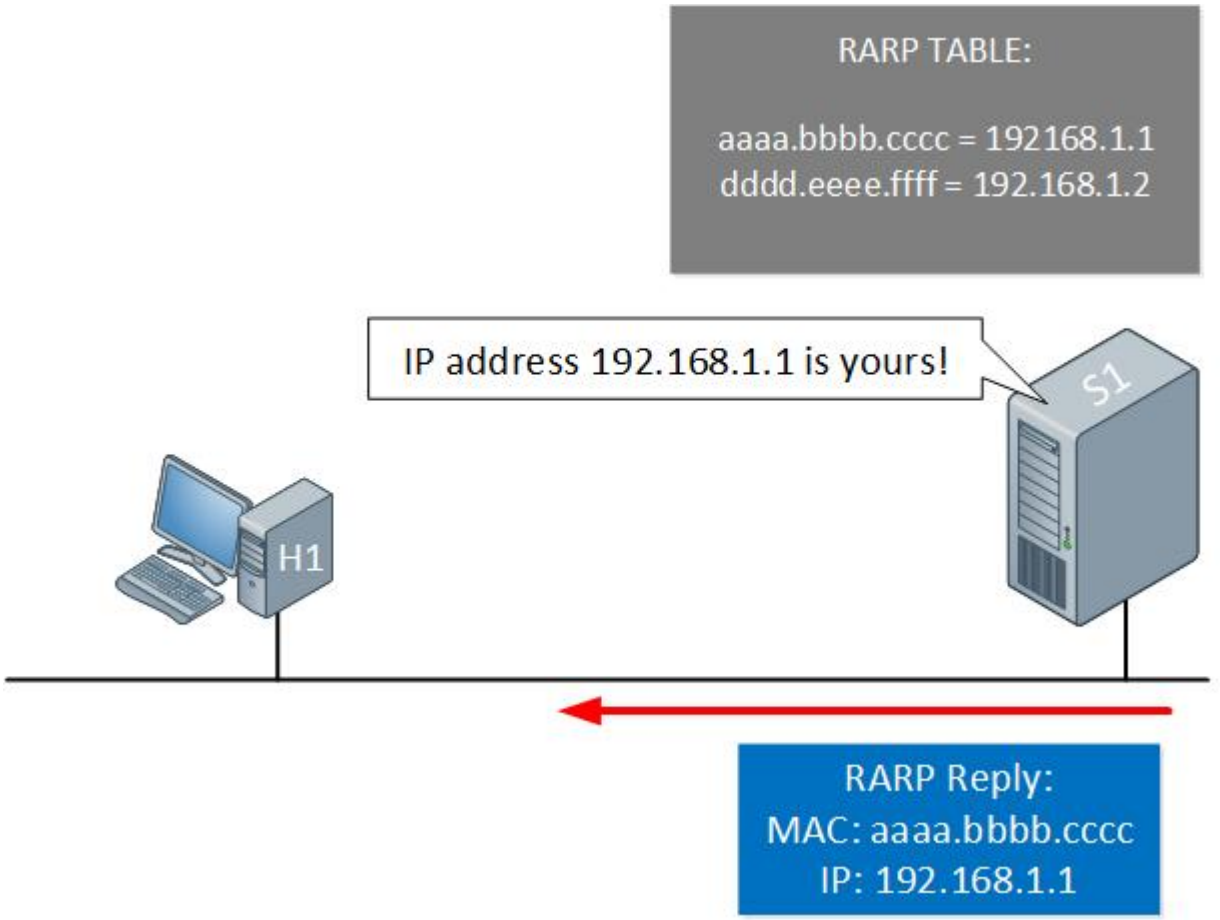


حلول أخرى للتخصيص الديناميكي للعناوين

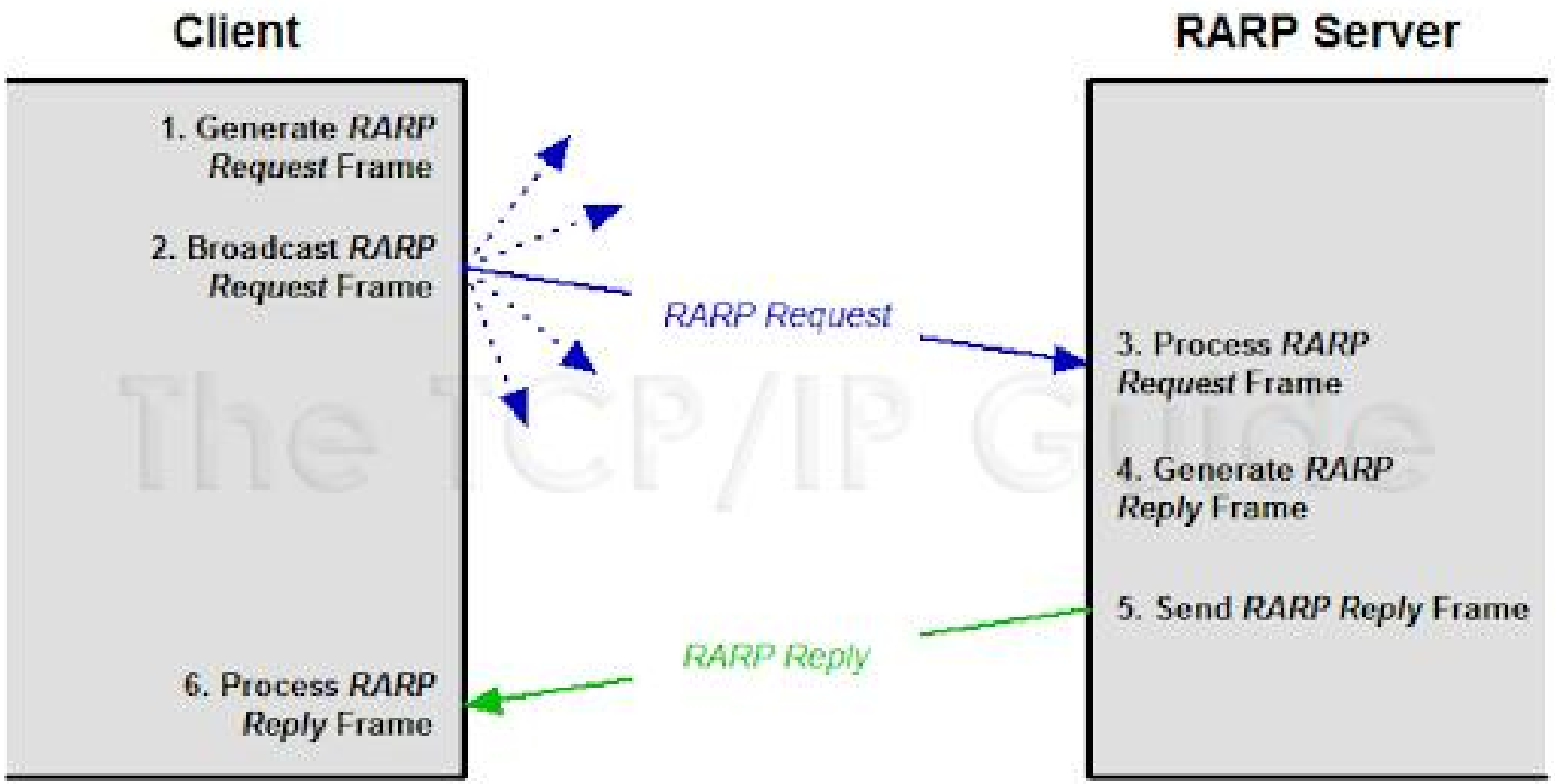
- RARP



حلول أخرى للتخصيص الديناميكي للعناوين



حلول أخرى للتخصيص الديناميكي للعناوين



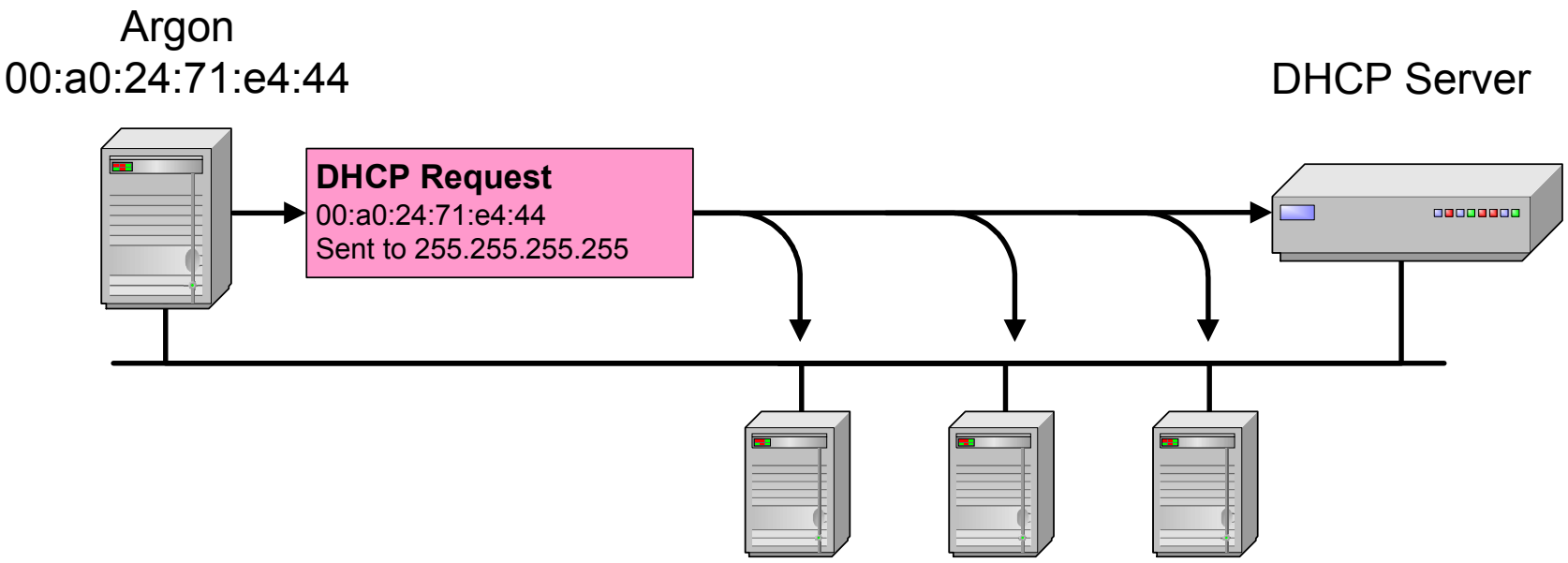
حلول أخرى للتخصيص الديناميكي للعناوين

- بروتوكول BOOTstrap (BOOTP)
  - تم تصميمه عام 1985
  - يقوم بتخصيص عنوان IP وقت الإقلاع (at boot time)
  - يُقدّم ثلاثة خدمات
    - تخصيص عنوان IP (IP address assignment)
    - اكتشاف عنوان IP للمخدم (Detection of the IP address for a serving machine)
    - يحدد اسم الملف الواجب تشغيله عند الإقلاع (boot file name)
  - يقوم بالإضافة لعنوان IP بتخصيص default router, network mask, الخ
  - يستخدم بروتوكول UDP ((host) 68 and (server) 67 UDP Port)
  - يستخدم limited broadcast address (255.255.255.255)

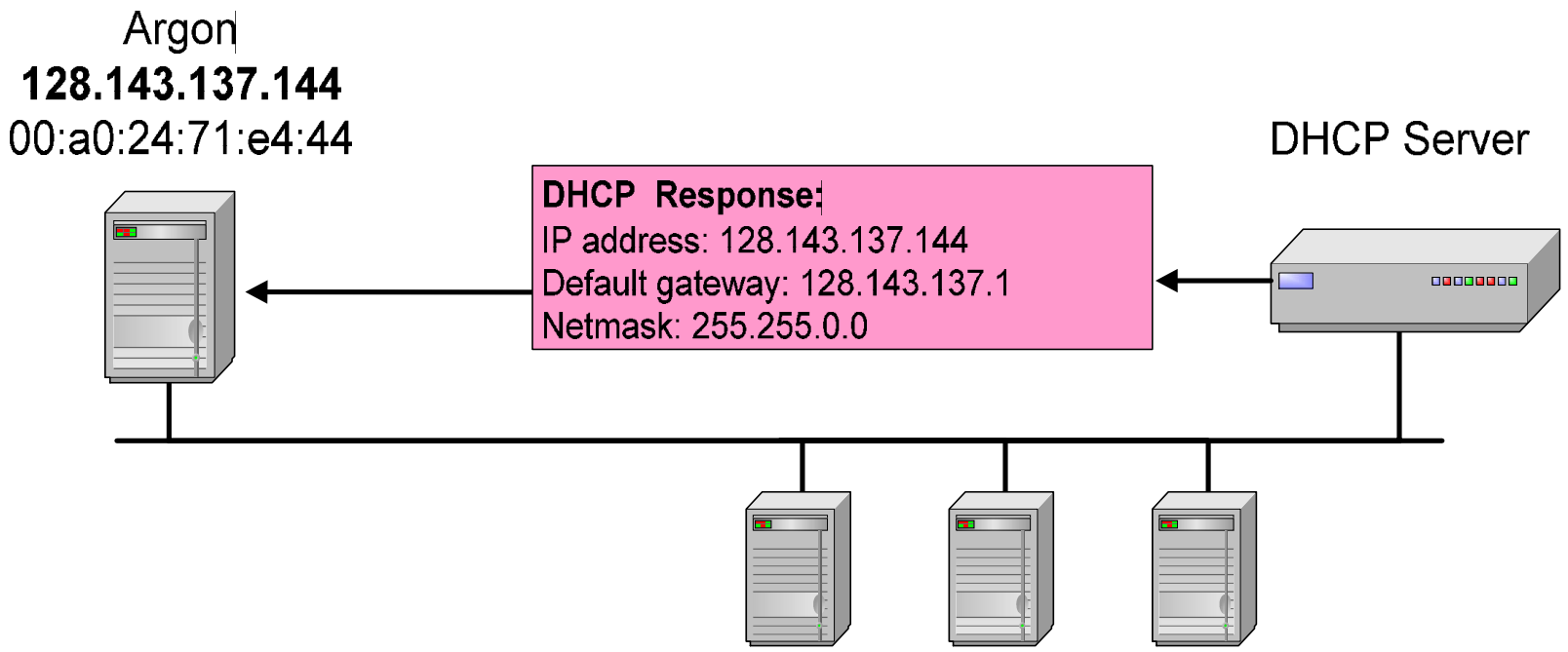
وظائف بروتوكول DHCP

- يقوم هذا البروتوكول بعدة وظائف, منها
  - تخصيص عناوين IP عند الحاجة (IP addresses are assigned on-demand)
  - تخصيص العناوين أوتوماتيكي
  - يدعم حركية الأجهزة (Support mobility of laptops)
  - تطوير لـ BOOTP
    - يدعم التخصيص المؤقت للعناوين (temporary allocation (“leases”) of IP addresses)
    - يقوم باختيار كامل إعدادات عنوان IP
  - يستطييع التواصل مع BOOTP clients

آلية عمل بروتوكول DHCP

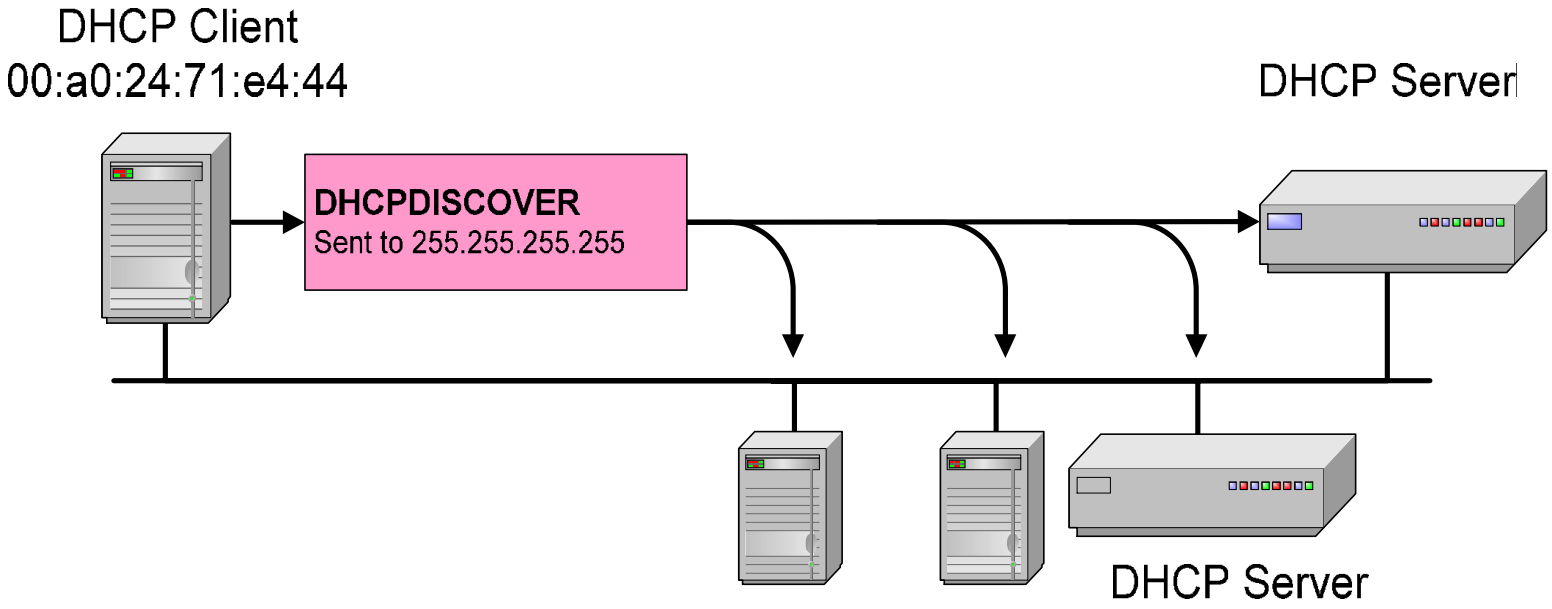


آلية عمل بروتوكول DHCP



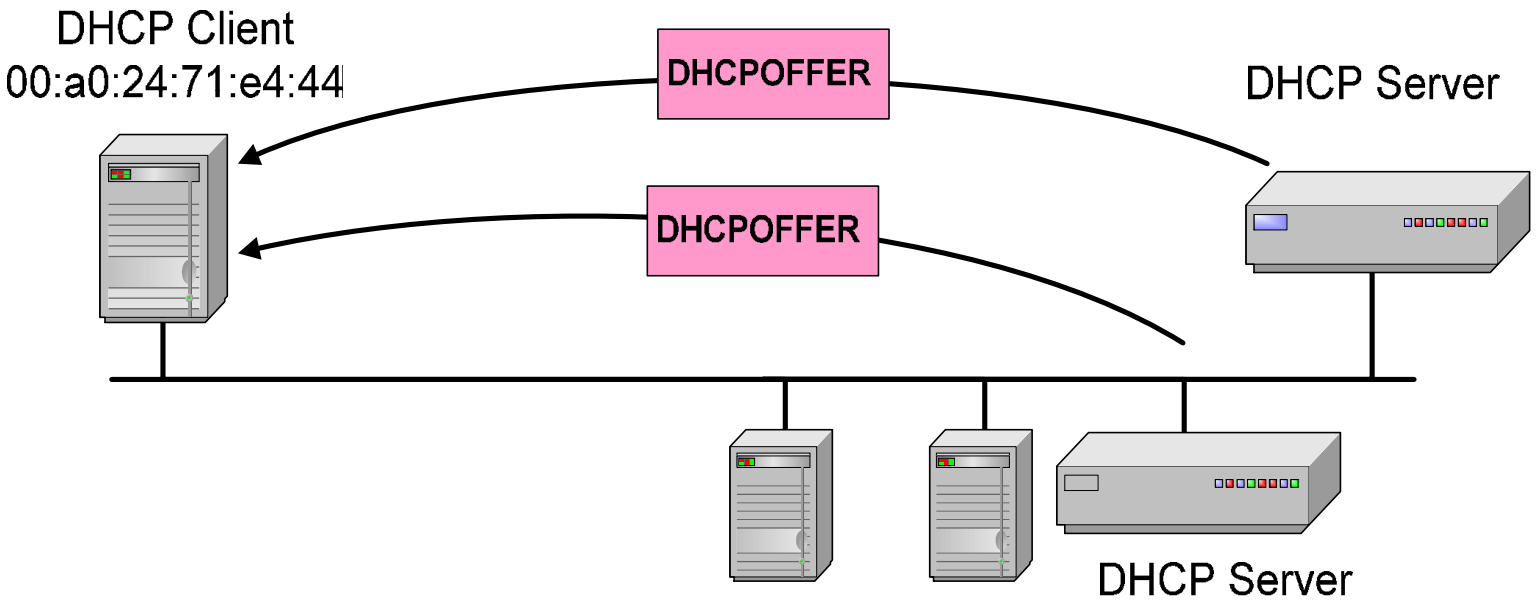
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- DCHP DISCOVER (the client does not know the IP address of DHCCP server)



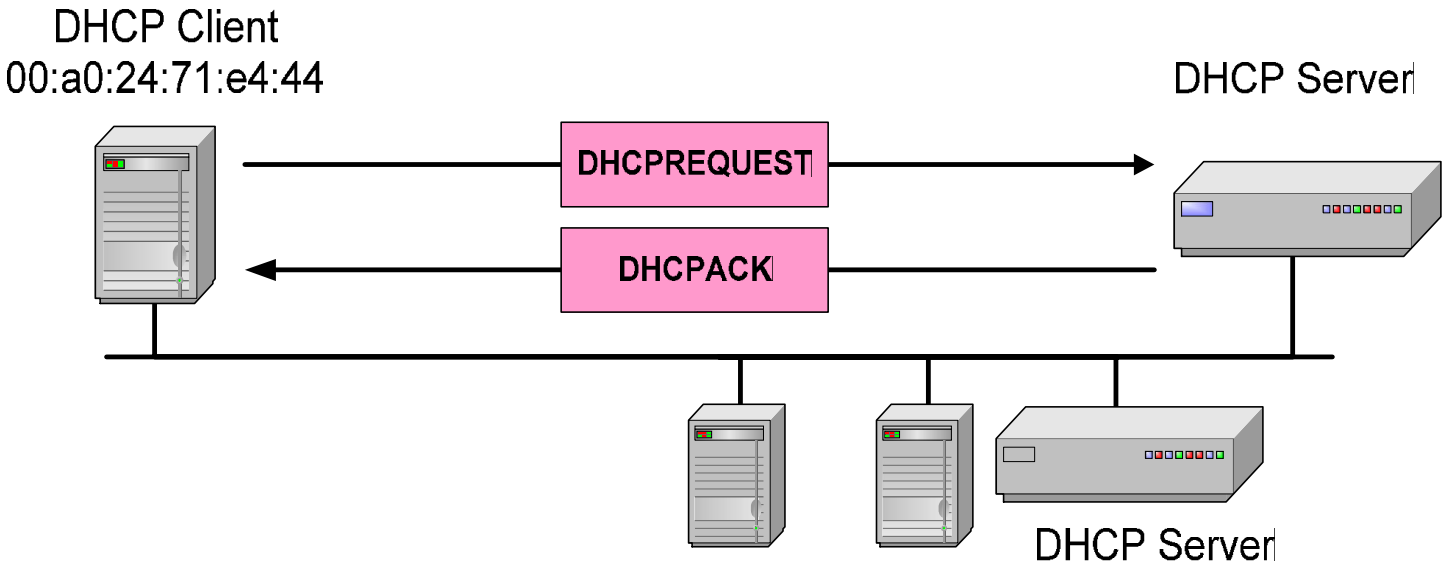
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- DCHP OFFER



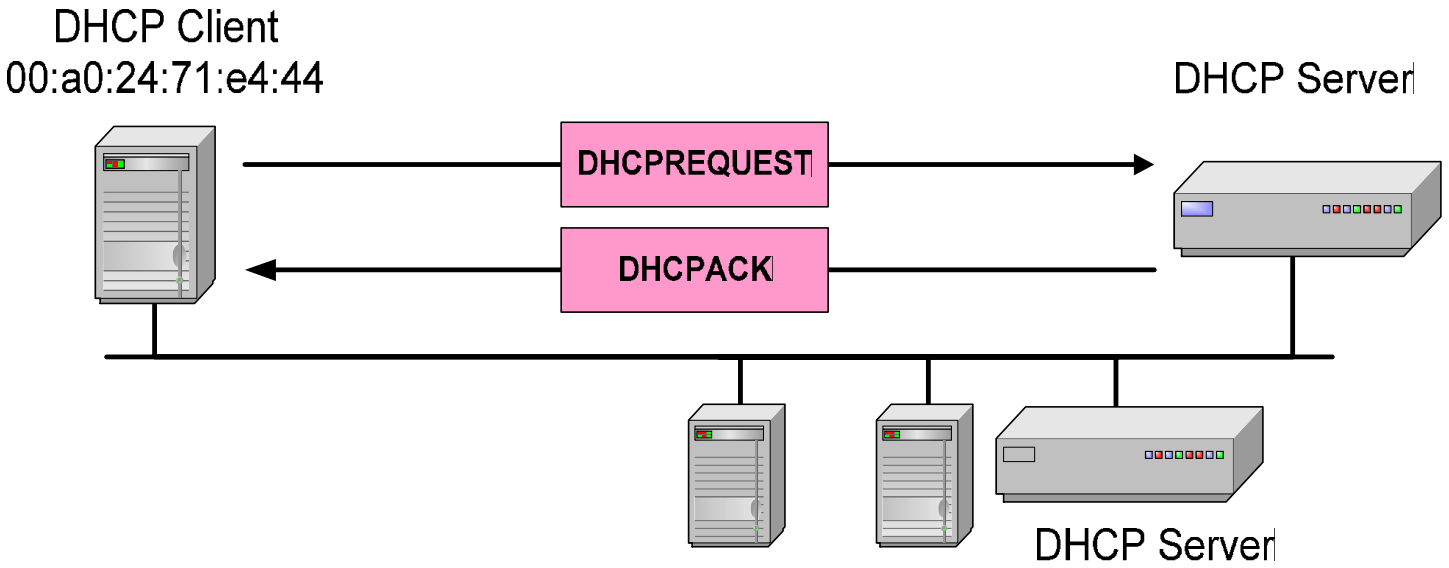
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- DCHP DISCOVER (the client knows the IP address of DHCCP server)



آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

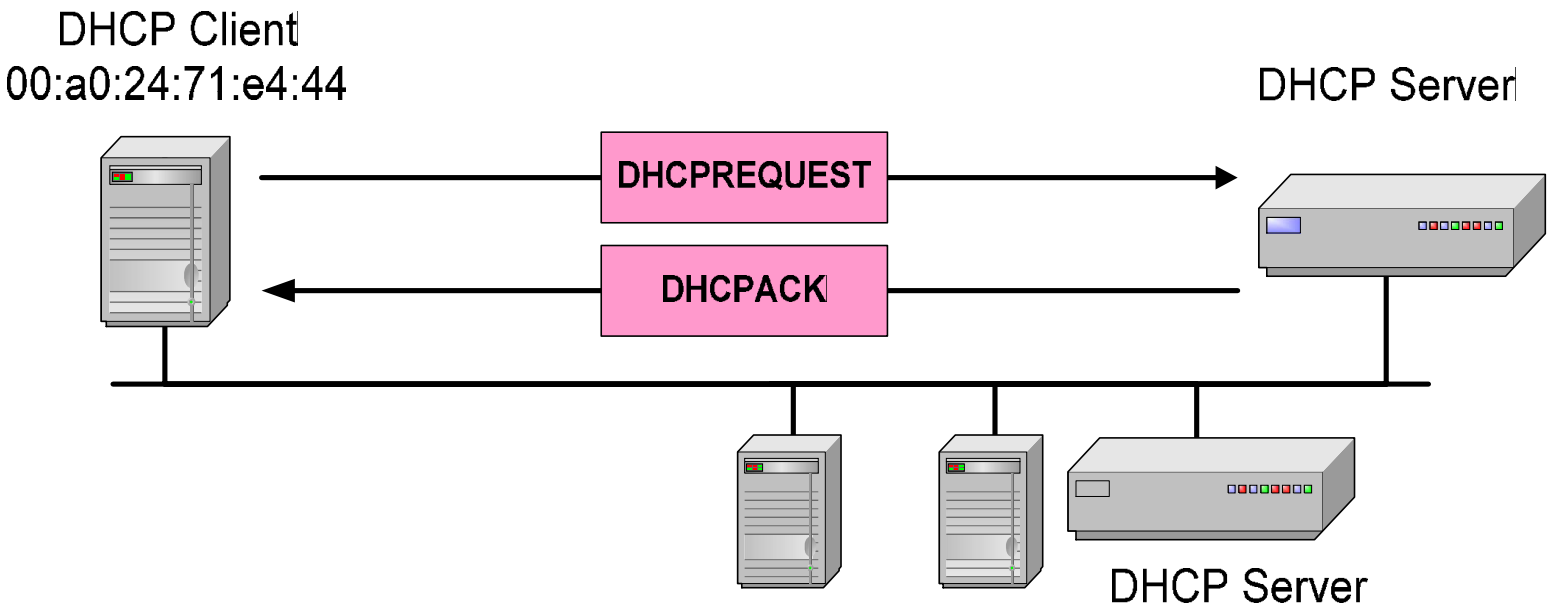
- DCHP DISCOVER (the client knows the IP address of DHCCP server)



At this time, the DHCP client can start to use the IP address

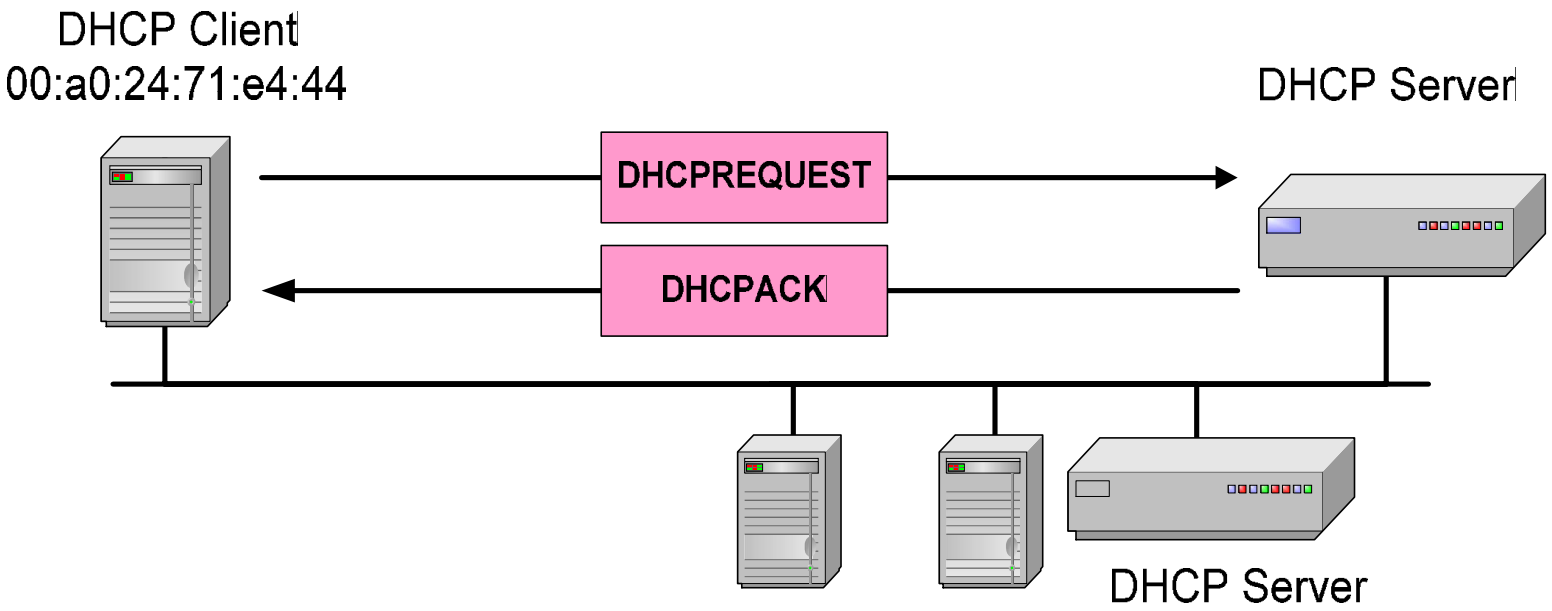
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- Renewing a Lease (sent when 50% of lease has expired)



آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

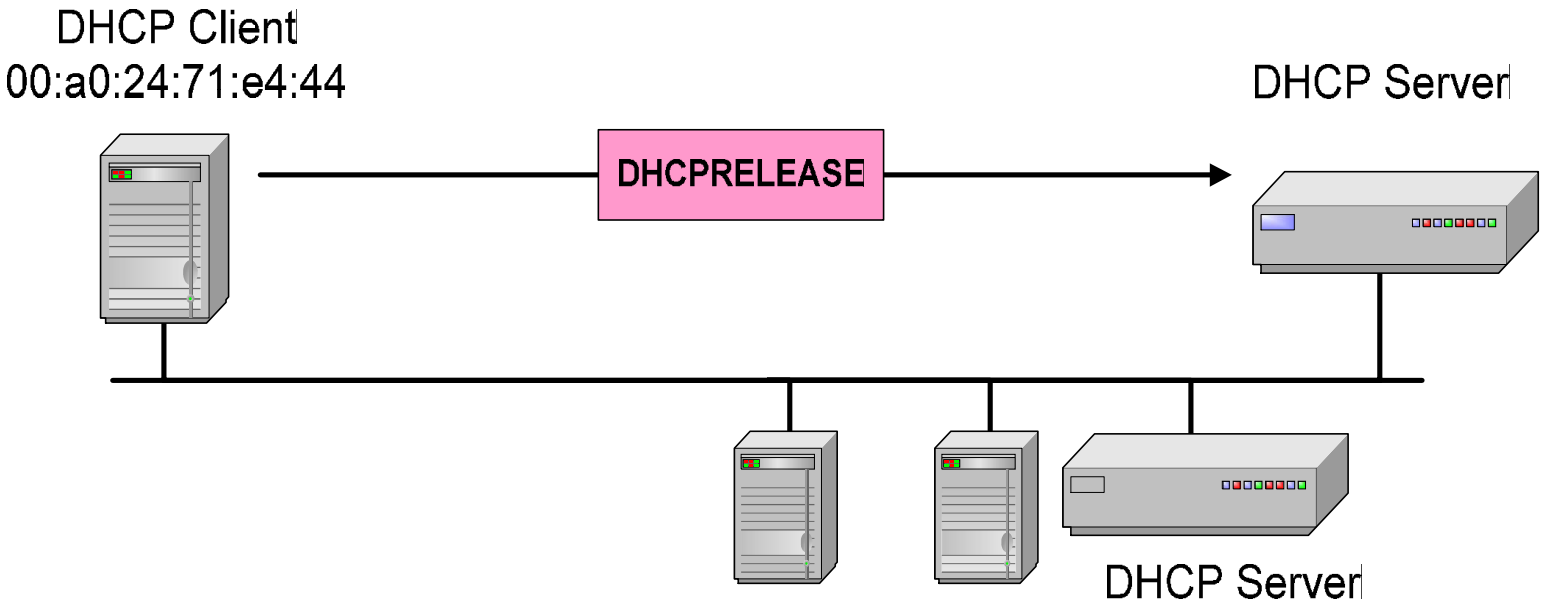
- Renewing a Lease (sent when 50% of lease has expired)



If DHCP server sends DHCPNACK, then address is released

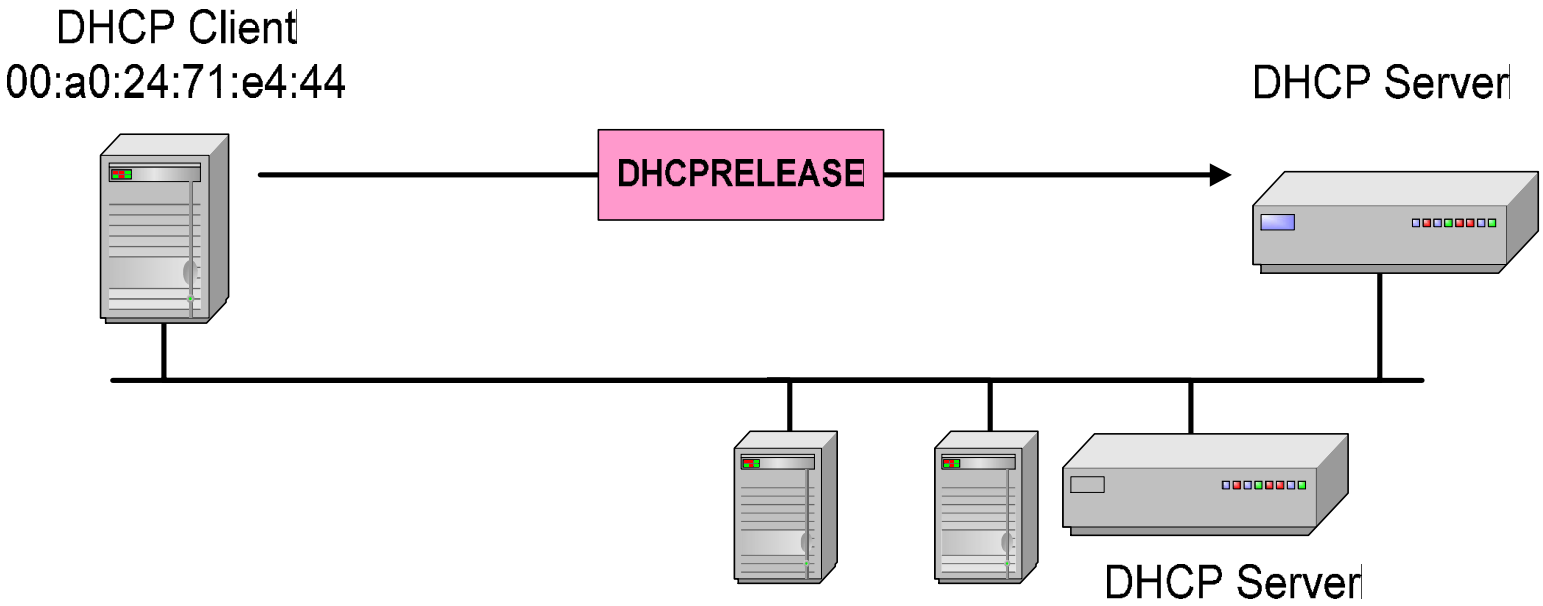
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- Renewing Release



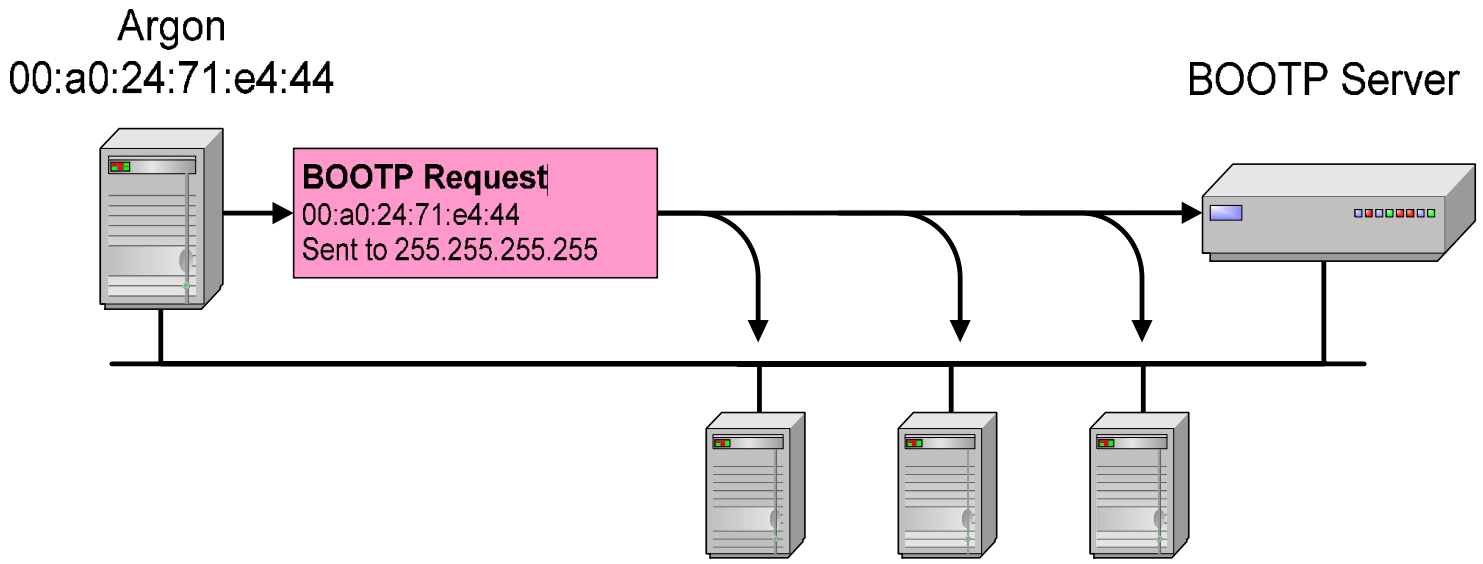
آلية عمل بروتوكول DHCP (نظرة أكثر تفصيلاً)

- Renewing Release

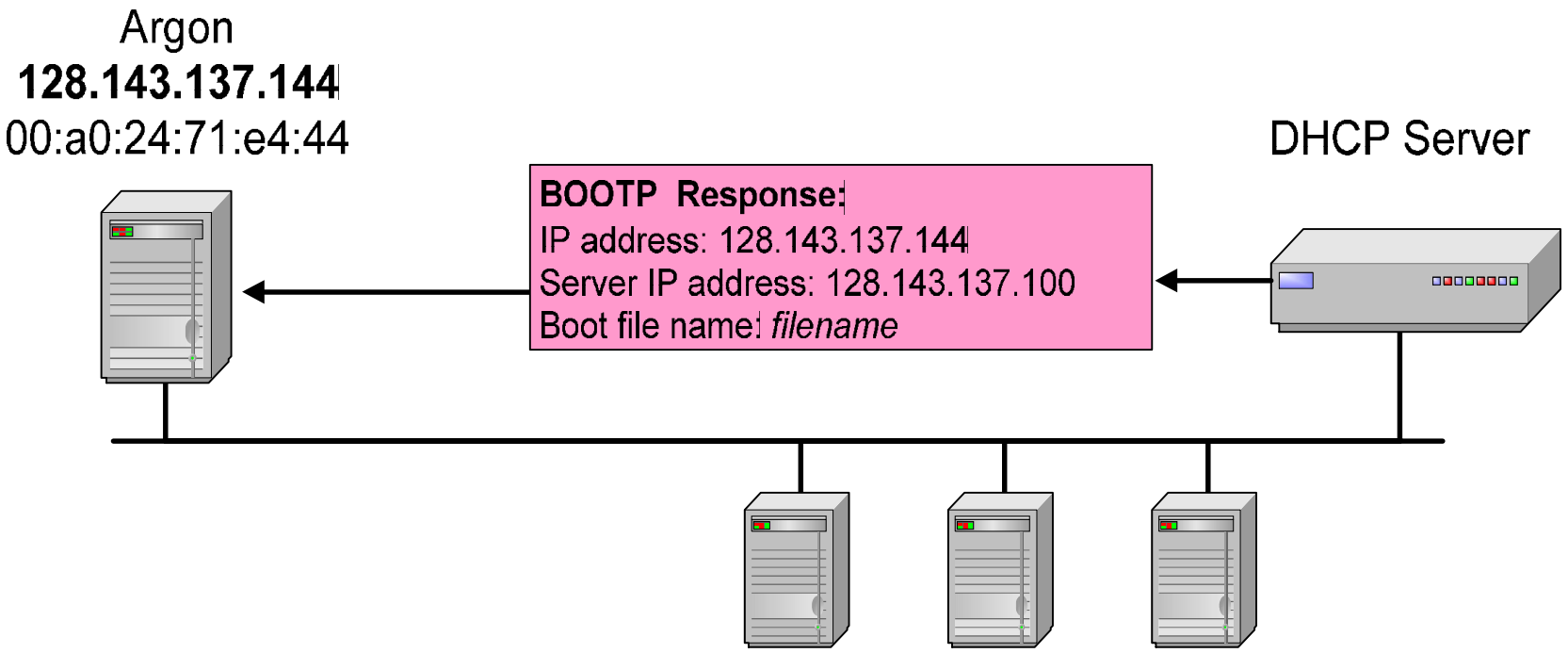


At this time, the DHCP client has released the IP address

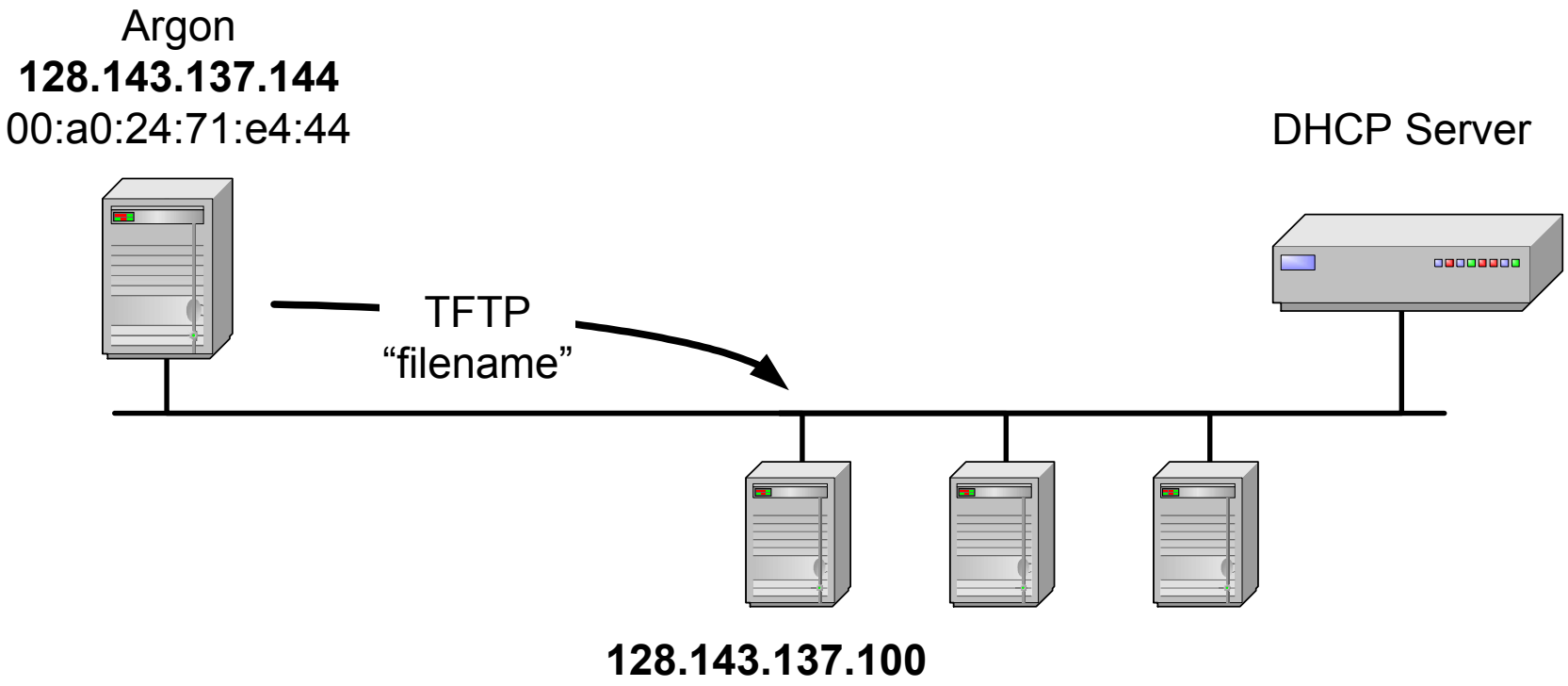
آلية عمل بروتوكول DHCP مع بروتوكول BOOTP



آلية عمل بروتوكول DHCP مع بروتوكول BOOTP



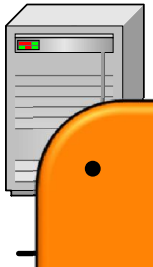
آلية عمل بروتوكول DHCP مع بروتوكول BOOTP

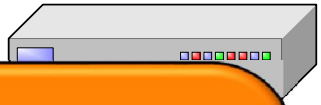


آلية عمل بروتوكول DHCP مع بروتوكول BOOTP

Argon
128.143.137.144
00:a0:24:71:e4:44

DHCP Server





- BOOTP can be used for downloading memory image for diskless workstations
- Assignment of IP addresses to hosts is static

IntServ

Integrated Service Architecture (IntServ)

- محدد في RFC 1633

- يهدف إلى تزويد تطبيقات الزمن الحقيقي (real-time applications) بضمانات حول جودة الخدمة (QoS guarantees)
  - لاتقدم الإنترنت, كما جرى تصميمها بشكل أساسي, لا تُعطي ضمانات لجودة الخدمة. أي يتم إرسال البيانات اعتماداً على مبدأ best effort

- Per-flow QoS model
  - يقسم IntServ الـ traffic إلى flows
    - كل flow عبارة عن تدفق من الباكيتات يتطلب جودة خدمة معينة, و كل flow محدد بـ 5-tuple "IP source address, IP destination address, protocol, TCP/UDP source port and TCP/UDP destination port"

Integrated Service Architecture (IntServ)

- الراوترات التي تدعم خدمة الـ IntServ (IntServ-enabled router)
تدعم تابعين أساسيين
  - Traffic control
  - Resource reservation

- Traffic control
  - Packet scheduler
    - يدير توجيه البيانات عبر مجموعة من الصفوف (queues)
  - Packet classifier
    - يقوم بتصنيف الباكيتات القادمة
    - يتم معالجة الباكيتات التابعة لنفس الصنف نفس المعالجة حتى لو لم يكونوا تابعين لعدة flows.
    - يتم تصنيف الباكيتات في كل موجه بناءً على معايير خاصة ضمن كل موجه (routers may classify their traffic differently)

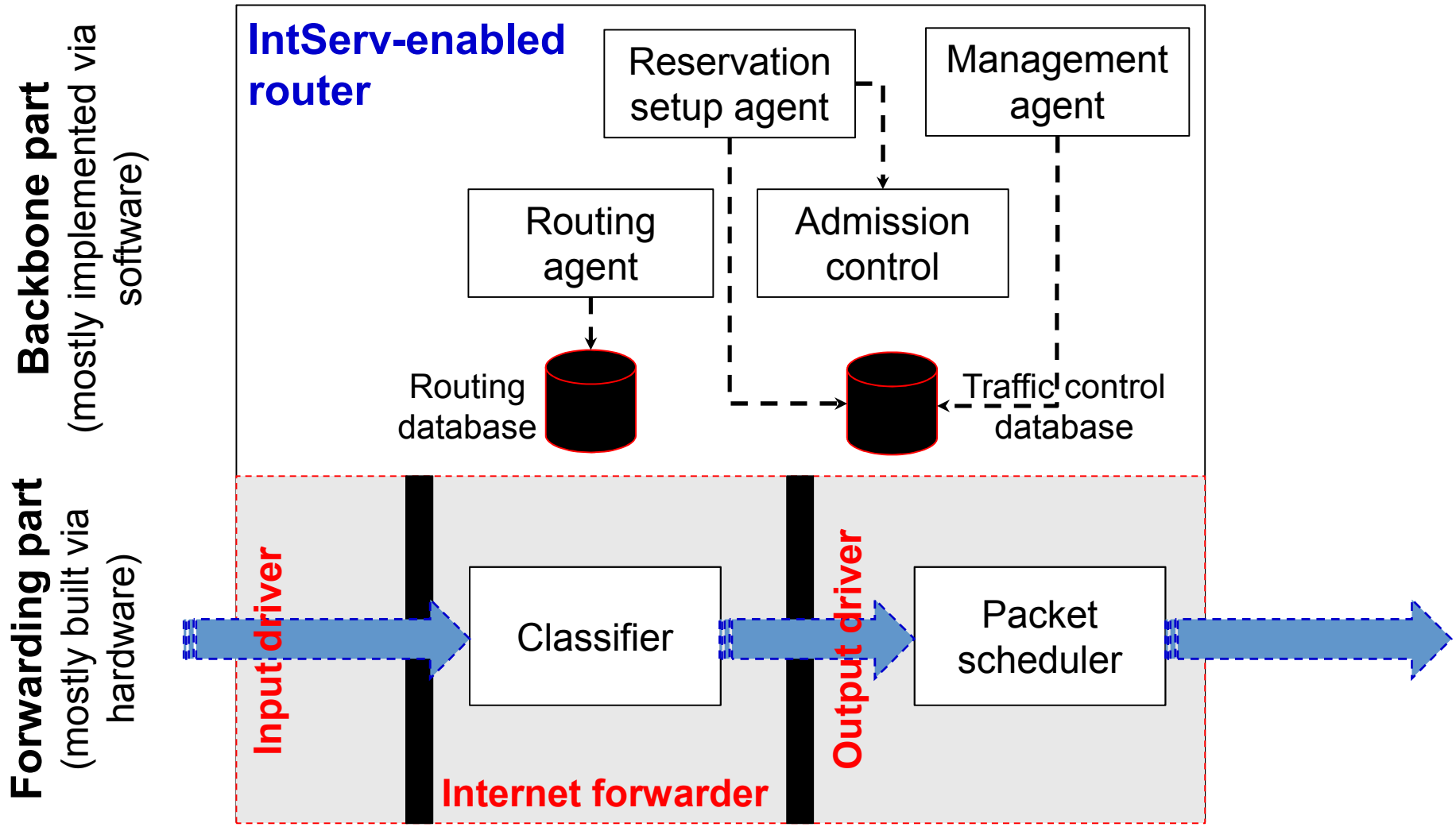
Integrated Service Architecture (IntServ)

- Admission control
  - يحدد فيما إذا كان الطلب الجديد يمكن أن يتم تخديمه أو لا بدون الإساءة للطلبات التي يتم تخديمها حالياً
  - يتم وضع هذه الخاصة في كل موجه, ليقوم باتخاذ القرار بقبول الطلب الجديد أو رفضه

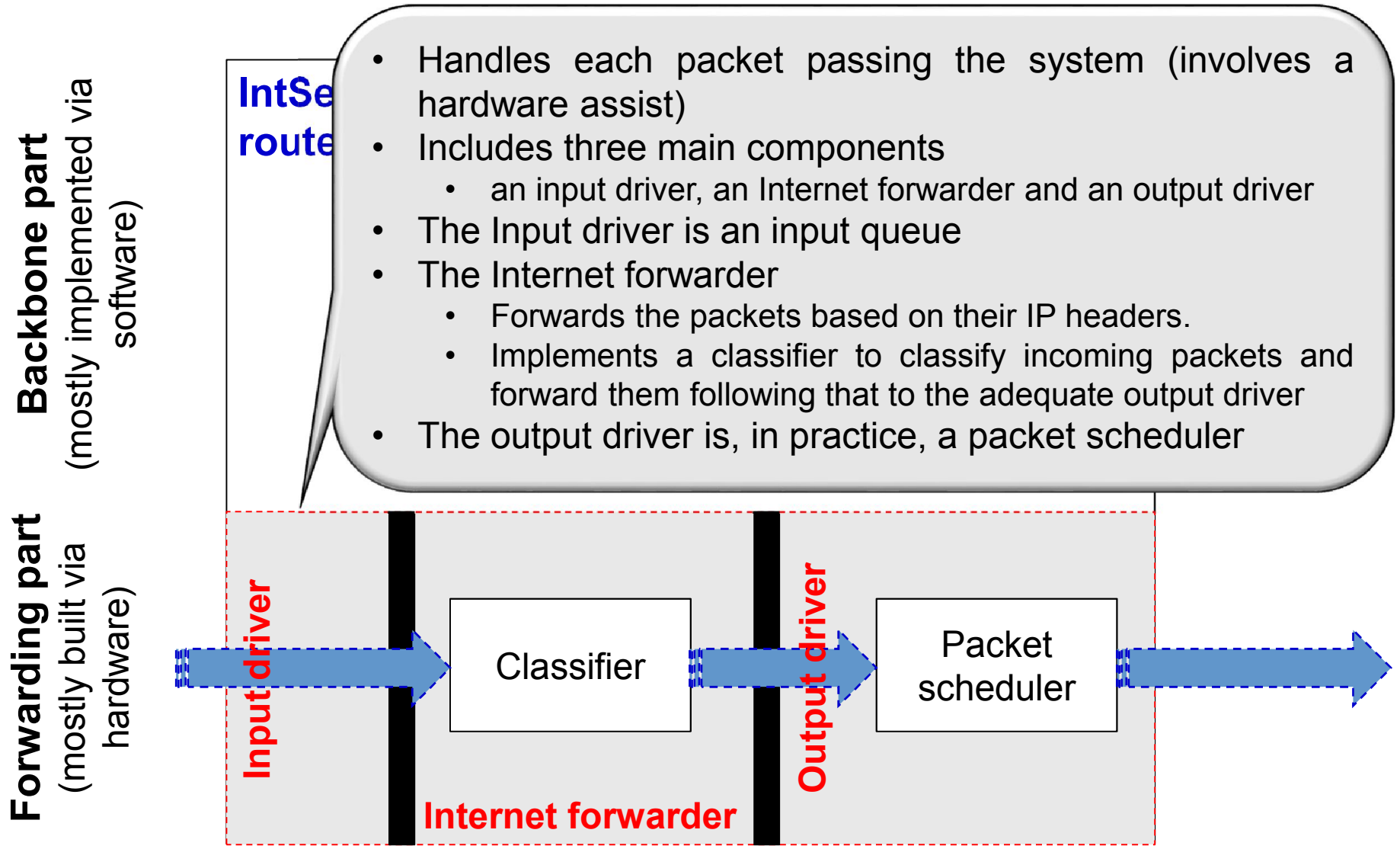
- Resource reservation
  - يتم تنفيذه بواسطة بروتوكول خاص للحفاظ على flow-specific states في الطرفيات و في كل موجه على طول الطريق من المرسل للمستقبل

- Standard protocol is the Resource reSerVation Protocol (RSVP)

Integrated Service Architecture (IntServ)

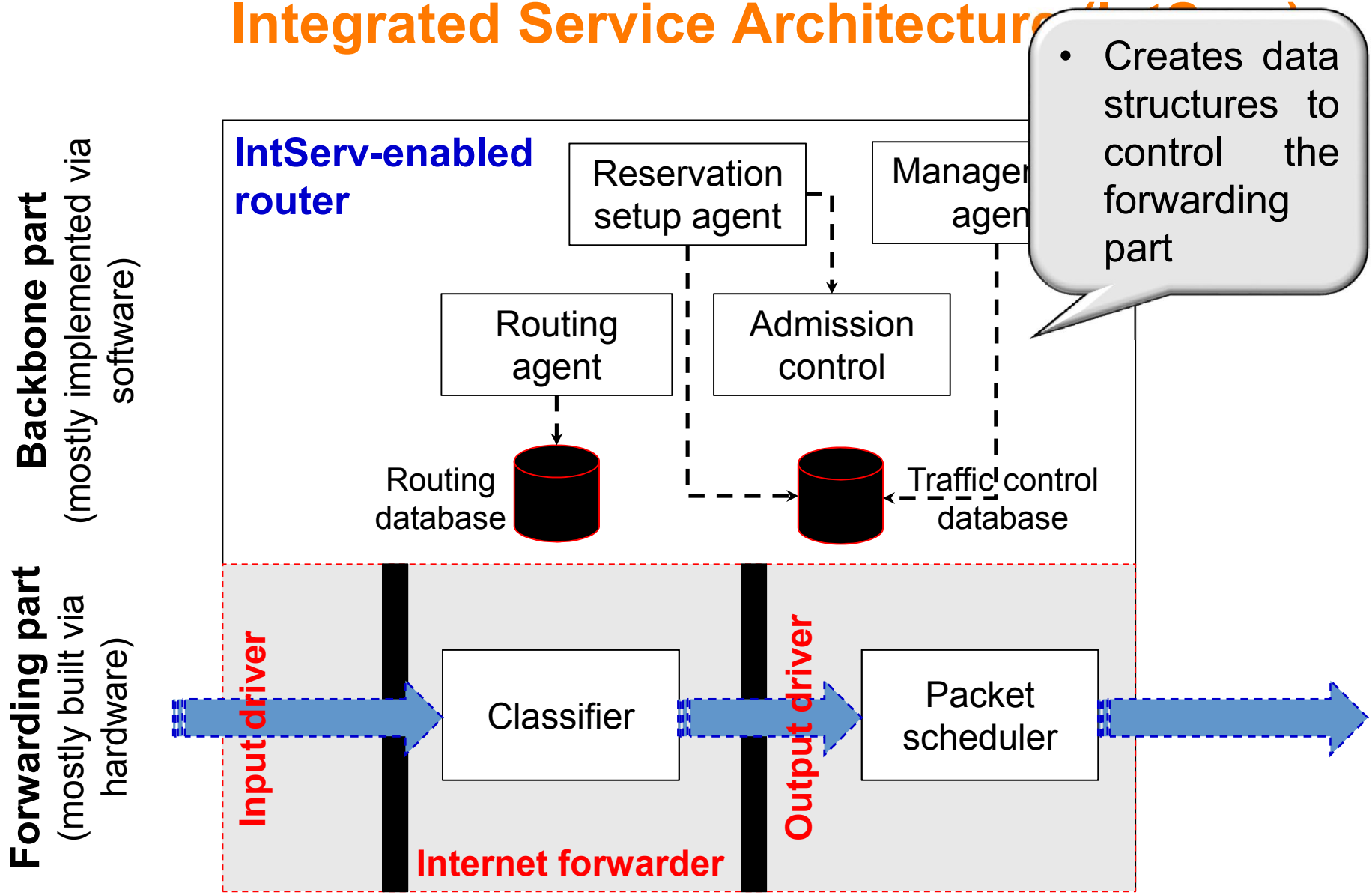


Integrated Service Architecture (IntServ)

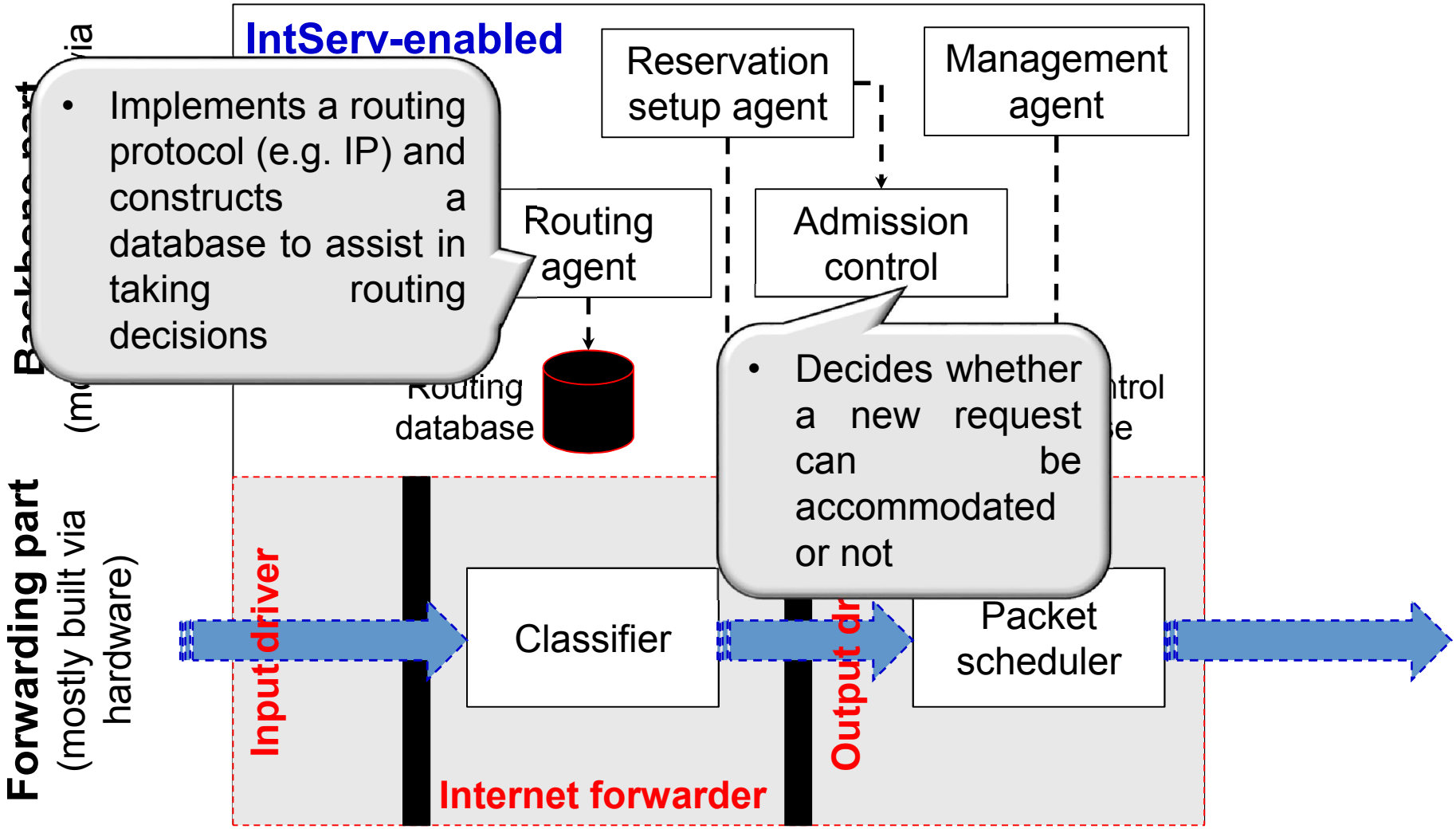


- Handles each packet passing the system (involves a hardware assist)
- Includes three main components
  - an input driver, an Internet forwarder and an output driver
- The Input driver is an input queue
- The Internet forwarder
  - Forwards the packets based on their IP headers.
  - Implements a classifier to classify incoming packets and forward them following that to the adequate output driver
- The output driver is, in practice, a packet scheduler

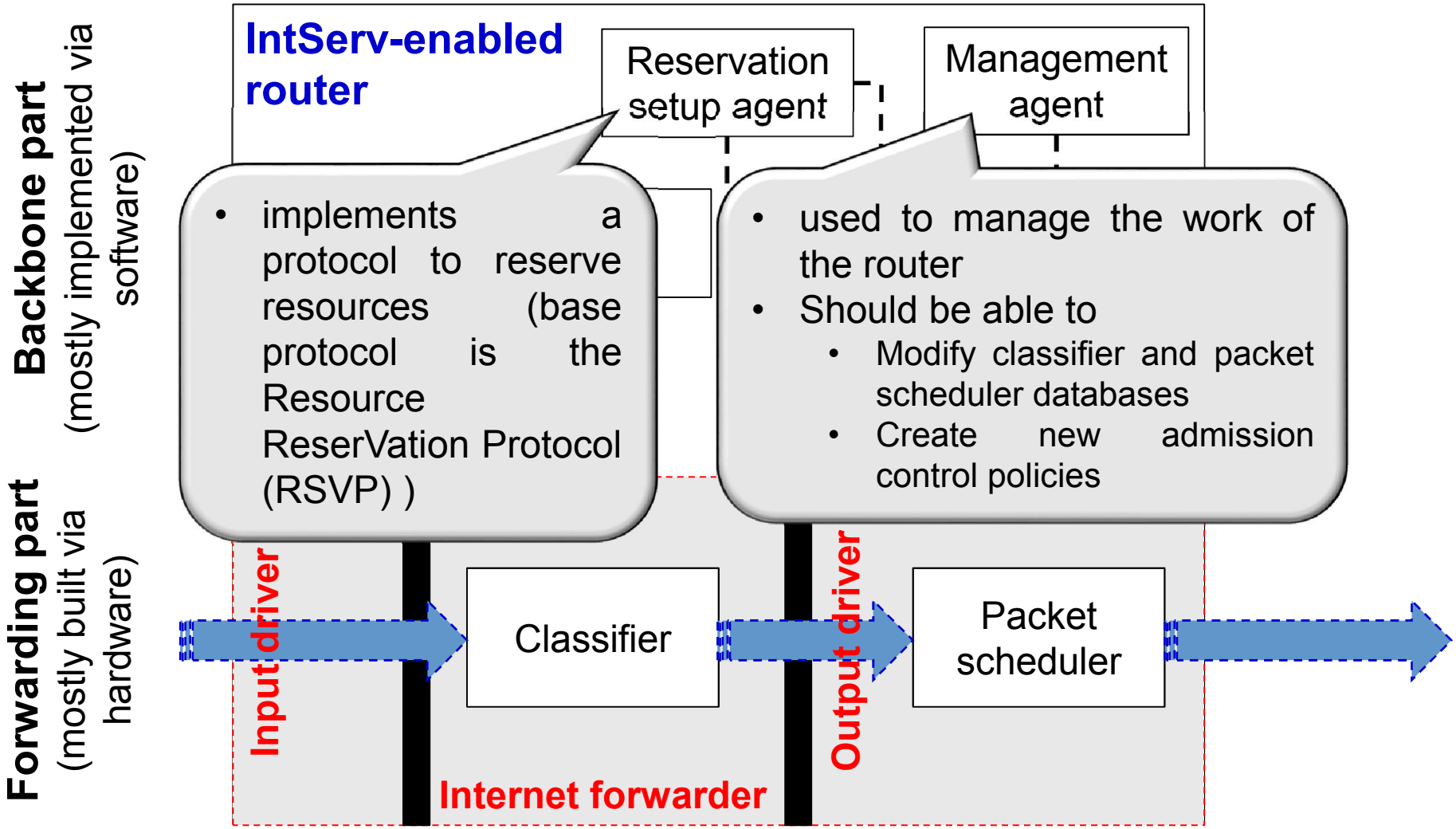
Integrated Service Architectur



Integrated Service Architecture (IntServ)

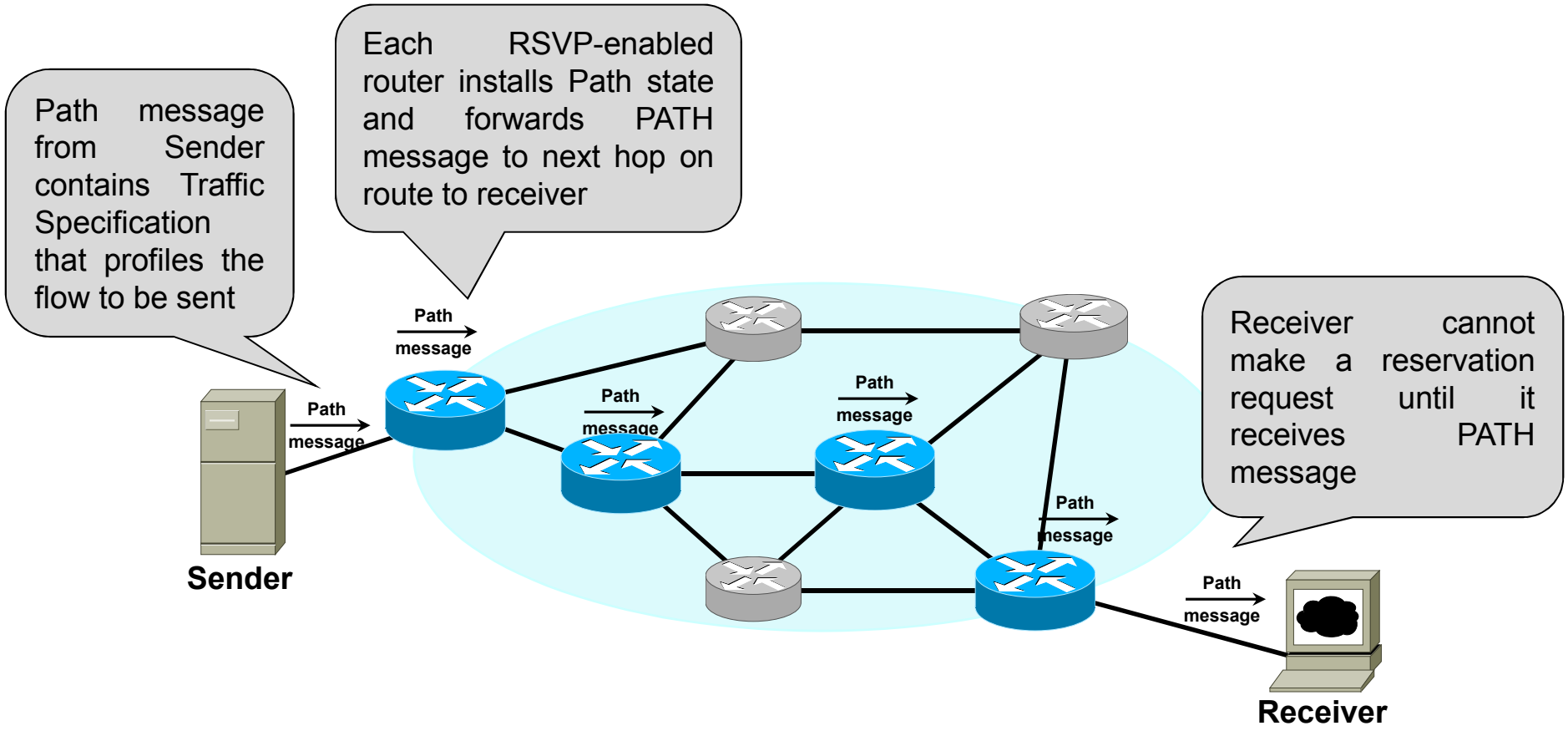


Integrated Service Architecture (IntServ)

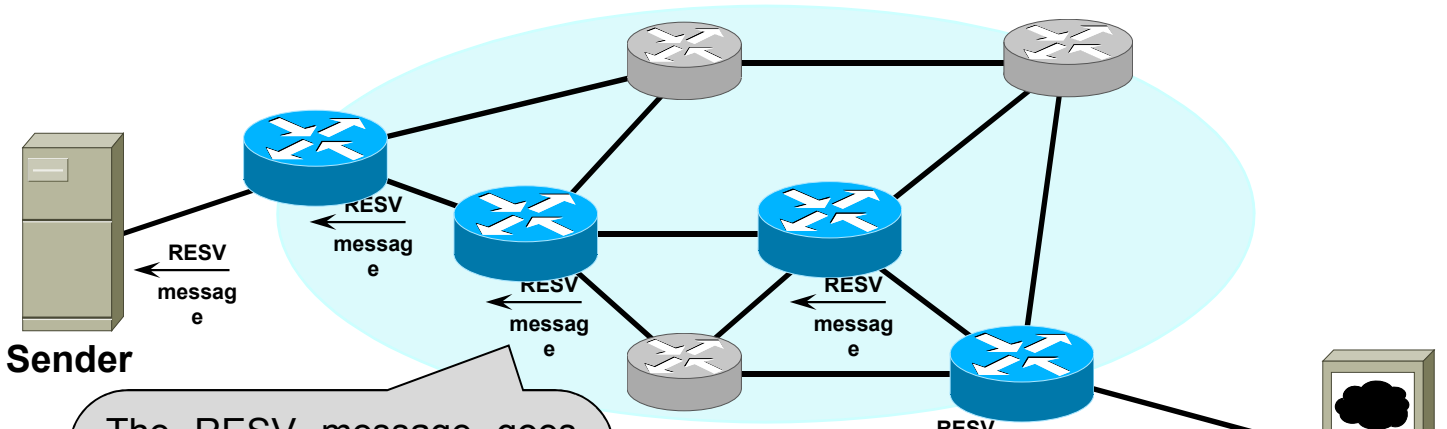


RSVP

Resource ReserVation Protocol (RSVP)



Resource ReserVation Protocol (RSVP)



The RESV message goes upstream following the Source Route provided in PATH message; each RSVP-enabled router makes the requested reservation

RESV message contains resource reservation request

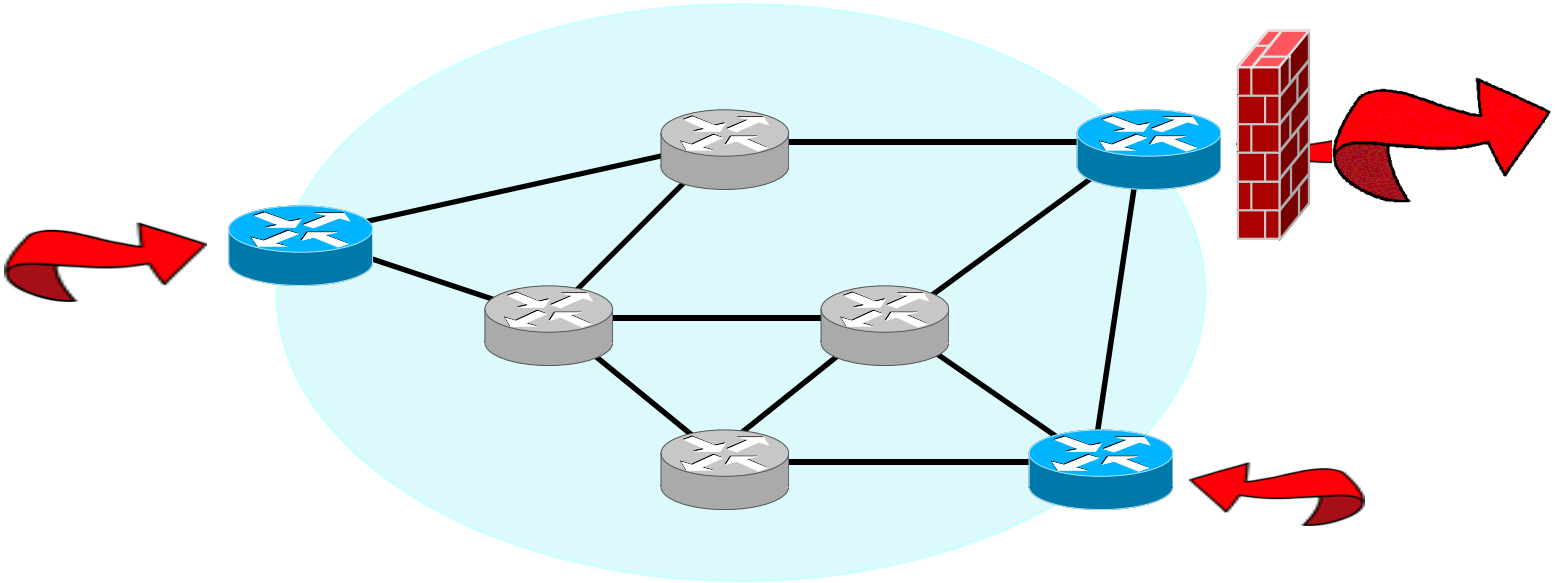
IntServ – Pros and Cons

- Pros
  - Provides the **highest possible level** of QoS
  - **Soft-states** behavior enables the release of resources after timeout even without explicit resource release messages
  - Supports a wide variety of applications
- Cons
  - Scalability problem
    - Each flow must be handled and maintained by each router on the data path
  - Signaling overhead due to RSVP soft-state behavior
  - Shortest path routing (OSPF) may not be optimal
  - No fair distribution of limited resources among users (no fairness)
  - Violation of IP principle (states are stored in end-hosts and in each router on the path in between)

DiffServ

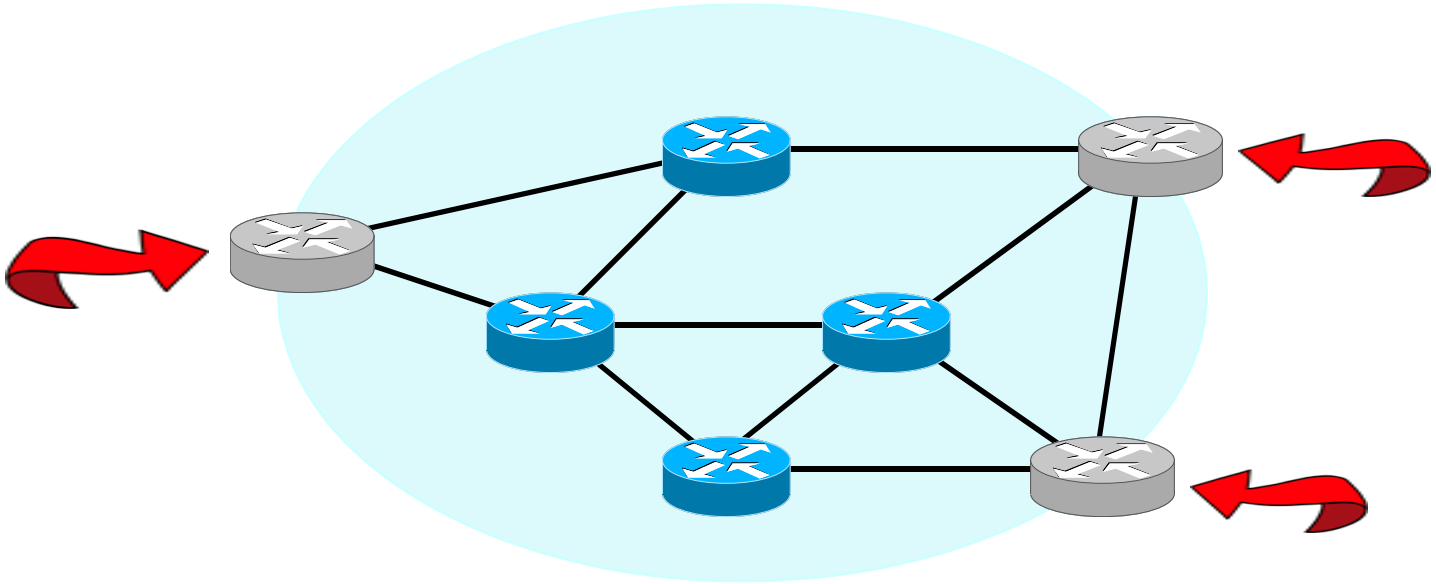
Differentiated Services Architecture (DiffServ) - Basics

- Edge routers
  - Forward customers traffic from/into the network –
  - Characterize, police, and/or mark traffic being admitted to the network –
  - Admission control –
  - Firewalls –



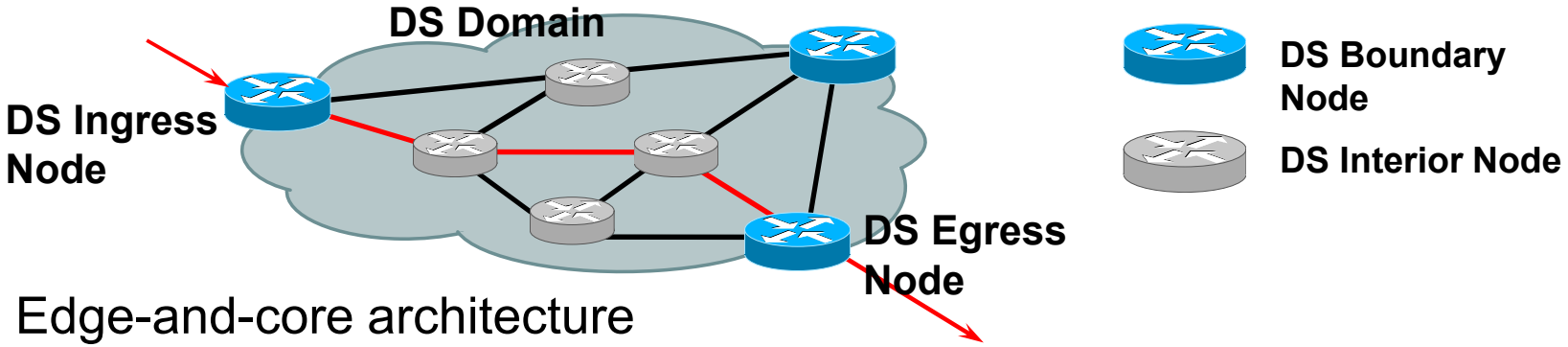
Differentiated Services Architecture (DiffServ) - Basics

- Core routers
  - Forward traffic between other core and/or edge routers
  - Differentiate traffic insofar to cope with transient congestion within the network
  - Intelligence is shifted to network borders (edge routers)



Differentiated Services Architecture (DiffServ) - Basics

- Ideas
  - Alternative to the high complexity of the IntServ architecture
  - Incremental improvements on the best-effort service model
  - Remove complexity from the core nodes → scalability



- Edge-and-core architecture
  - Complex decision making is pushed to the edges
  - Edge-to-edge are built from a small set of core router behaviors

DiffServ – Traffic Classification

- Two primary types of DiffServ classifiers (applied in ingress node)
  - Behavior Aggregate (BA)
    - Packet classification solely based on DiffServ field (Differentiated Services Code Point – DSCP values) in IP header (former ToS field)
  - Multi-Field (MF)
    - Packet classification based on multiple fields of the header
      - Source and destination addresses
      - Source and destination ports
      - Protocol ID
- Within a DiffServ domain many flows may share a single DSCP

DiffServ – Traffic Classification

- Per Hop Behavior (PHB) is a description of the externally observable forwarding behavior of a DiffServ node applied to a particular BA
  - Resources (buffer, bandwidth, etc.)
  - Priority relative to other PHBs
  - Relative observable traffic characteristics (delay, loss, etc.)

  No constraints with respect to implementation!

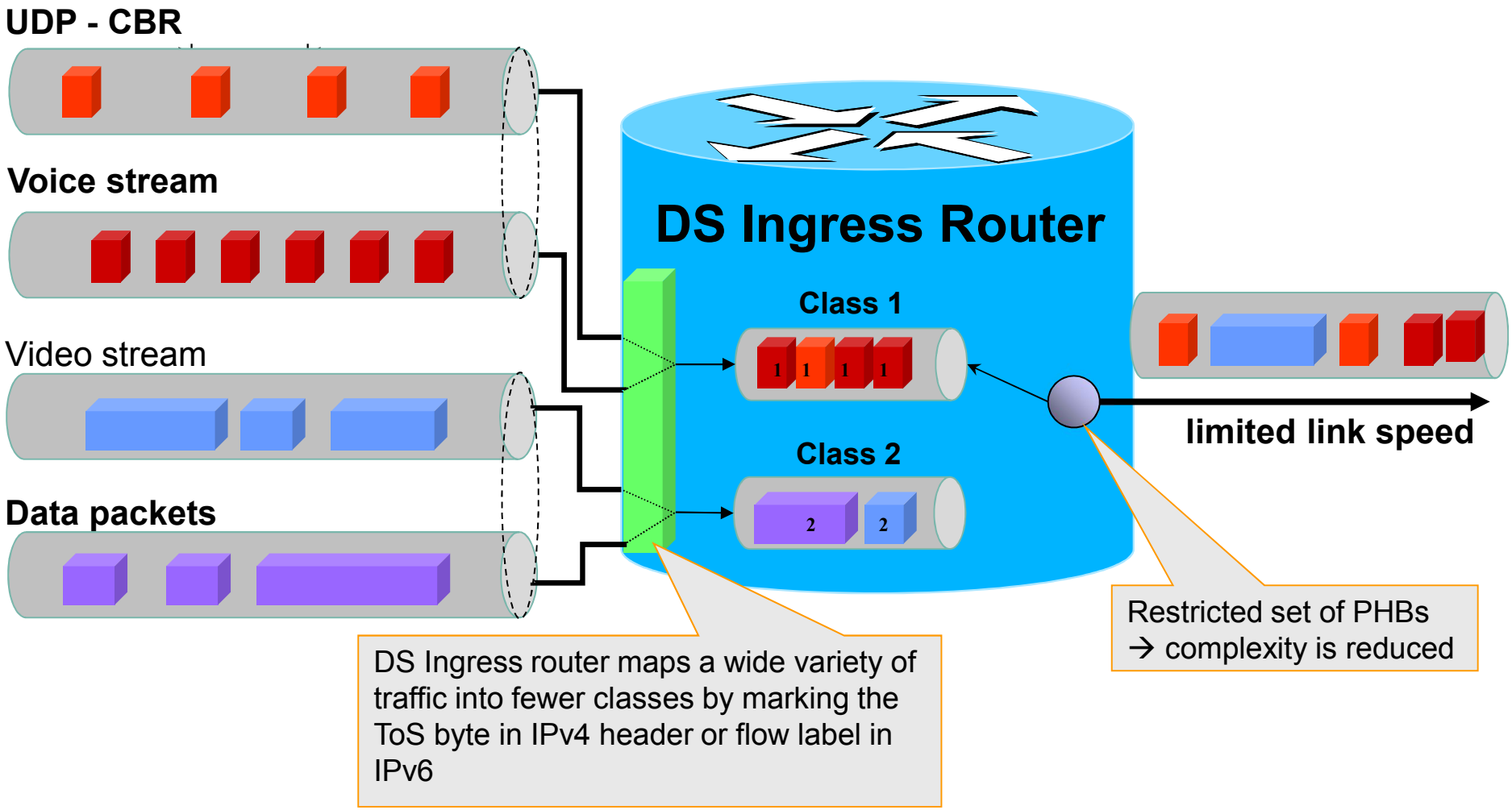
- PHBs are indicated by specific values in the DSCP and build blocks for edge-to-edge services
  – DiffServ allows to map multiple DSCP values onto the same PHB

DiffServ – Traffic Classification

- Two PHBs have been standardized by IETF
  - Expedited Forwarding (EF)
    - Every router along the path services EF packets at least as fast as the rate at which EF packets arrive
      - Rate shape or police EF traffic on entry to the DS Domain
      - Configure the EF packet-servicing interval at every core router to exceed the expected aggregate arrival rate of EF traffic
      - EF packet-servicing intervals must be unaffected by the amount of non-EF traffic waiting to be scheduled at any given instant
    - Used for
      - low-loss, low-latency and low-jitter services
  - Assured Forwarding (AF)
    - Relative bandwidth availability
    - Packet drop characteristics
    - Parameters (drop probabilities, queue sizes, etc.) are assigned by the network operator allowing him to build desired end-to-end services

DiffServ – Traffic Classification

Wide variety of E2E services



DiffServ – Pros and Cons

- Pros
  - Wide variety of services and simple introduction of new ones
  - Avoid per-flow or per-customer state handling within core network nodes → scalability
  - Interoperability with old network nodes
  - Support of incremental deployment
  - Division of forwarding path and management plane

- Cons
  - QoS guarantee is on the basis of PHB → difficult to predict E2E behavior, especially if packets cross many DiffServ clouds

Next Step In Signaling (NSIS)

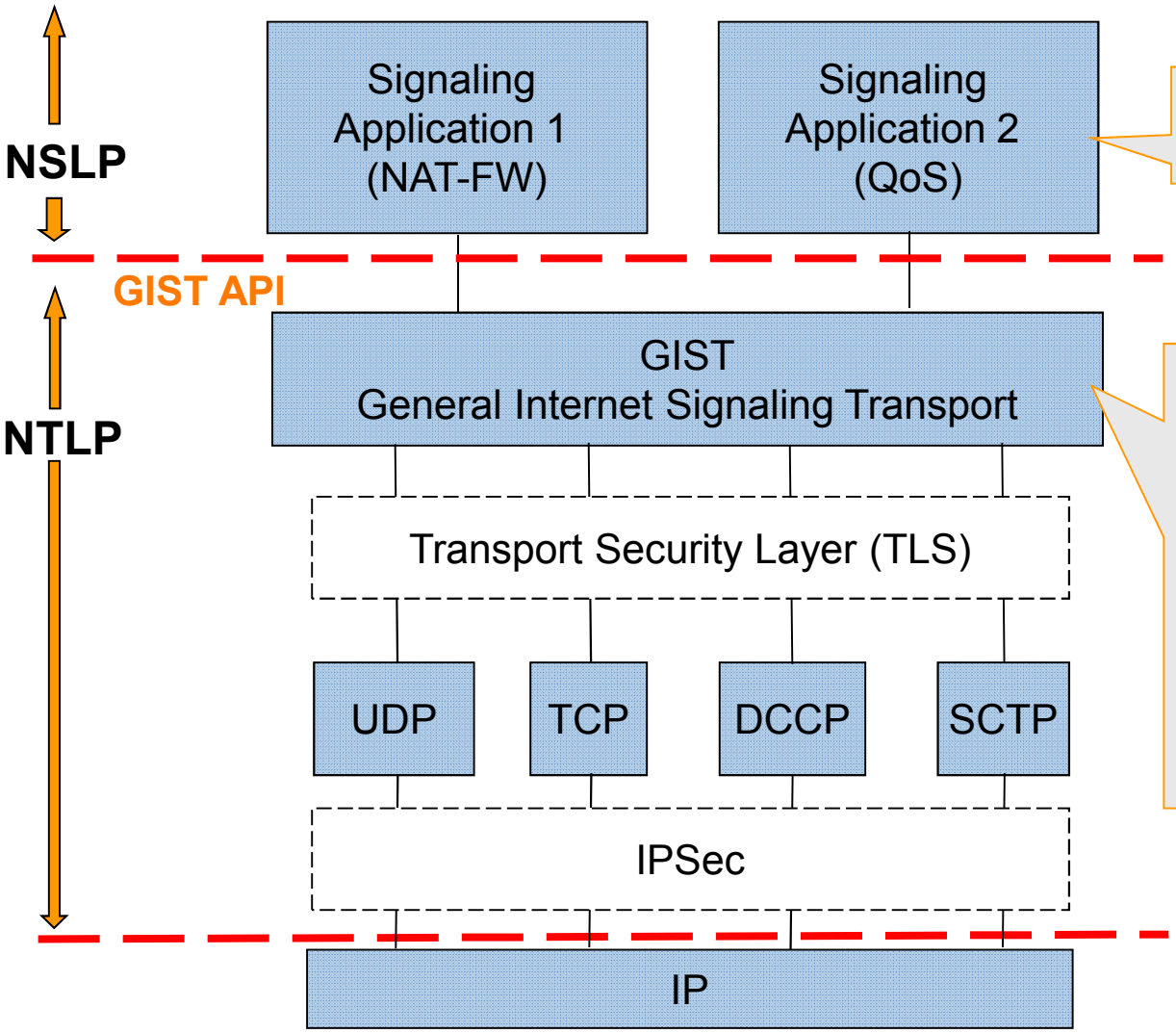
Next Step In Signaling (NSIS)

- Developed by the IETF nsis working group (RFC 4080)
- Framework aiming at
  - Interworking between different QoS mechanisms
  - Simplified QoS signaling
  - Support of mobility
- Same signaling problem RSVP are addressed. However
  - In contrast to RSVP, NSIS remains usable in different parts of the Internet without requiring a complete E2E deployment
  - Signaling can be used for purposes other than resources reservation

NSIS - Overview

- NSIS aims at providing a global model that supports several signaling applications by separating the protocol stack into two layers
  - NSIS Signaling Layer Protocol (NSLP)
    - Contains different signaling applications, e.g. QoS signaling, NAT, Firewall, etc.
    - Communicates with NTLP
  - NSIS Transport Layer Protocol (NTLP)
    - Interface between the NSLP and IP
    - GIST (General Internet Signaling Transport protocol)
      - Common signaling transport service for different signaling applications
      - Interacts with other security and transport protocols, e.g. TCP, IPSec, etc.

NSIS - Overview

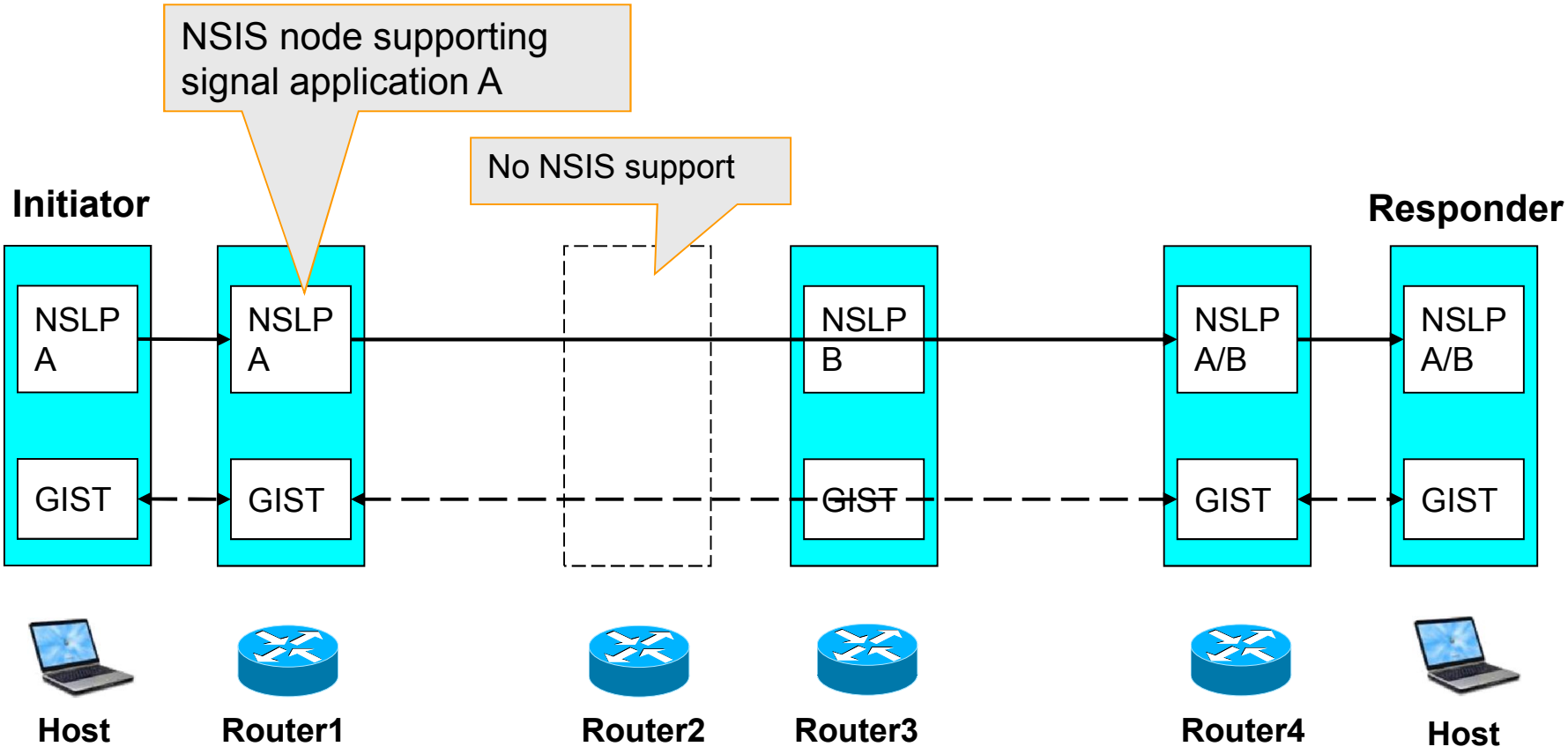


Signaling application-specific functionality

Routing of per-flow signaling messages

1. Discovery of next node
2. Transport of signaling message
3. Reusing of existing transport and security protocols

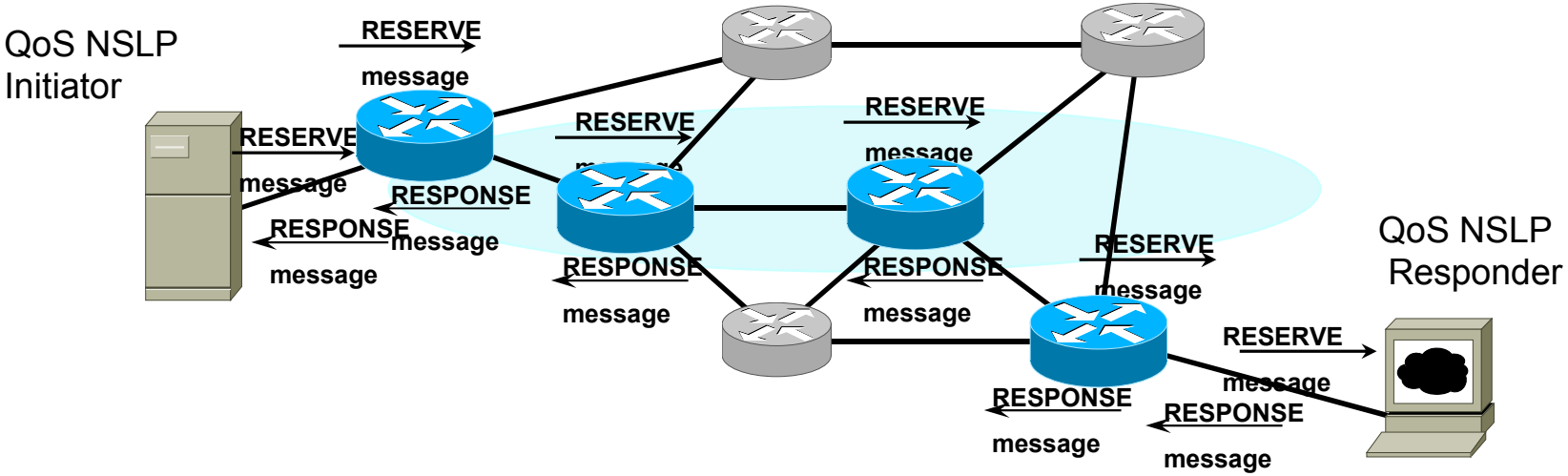
NSIS – NTLP/NSLP Scenario



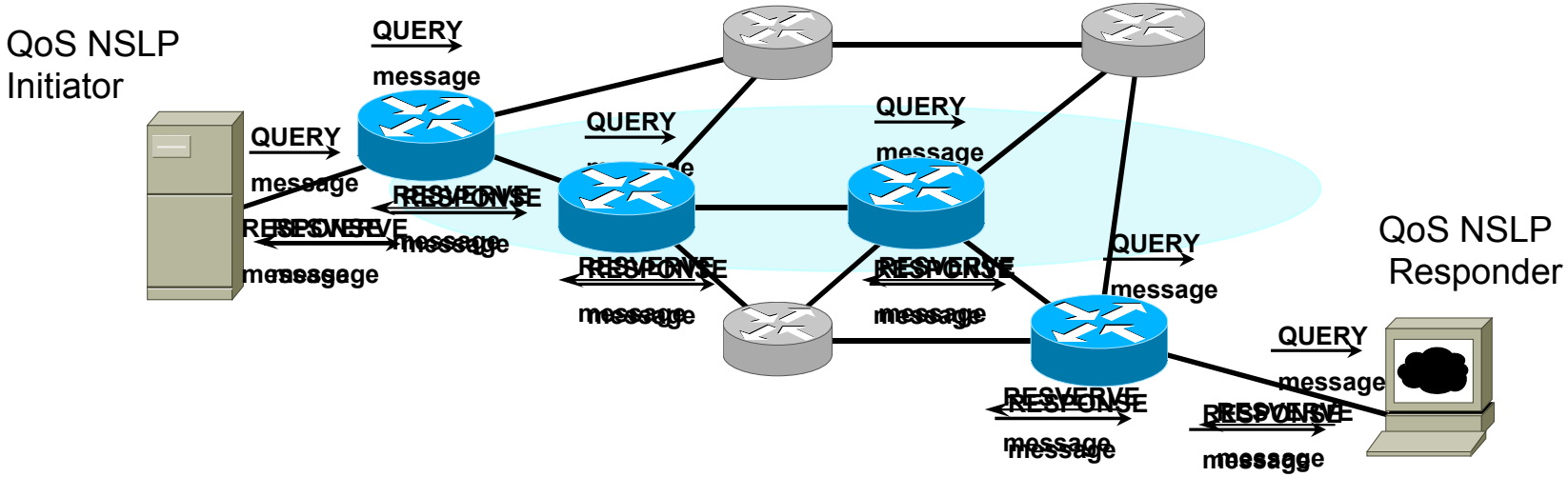
QoS – NSLP

- RSVP-like operation, however only unicast is supported
- Sender- and receiver-initiated reservations
- Support for different QoS models such as Intserv, Diffserv, others
- Four types of messages are used
  - RESERVE: creates, modifies or deletes reservation state
  - QUERY: discovers available resources along a certain path
  - RESPONSE: acknowledgement that indicates receiving RESERVE or QUERY
  - NOTIFY: notifies in case of errors

Sender-Initiated Reservation



Receiver-Initiated Reservation



NSIS – Pros and Cons

- Pros
  - Support of different signaling applications
  - Decoupling of discovery and transport of signaling messages
  - Flexible flows, each session has an ID
    - Session ID can be changed → support of mobility
  - Receiver- and sender-oriented reservation
  - Better Scalability and extensibility than other mechanisms
- Cons
  - More complex than other technologies
- **NSIS is now under development**

بروتوكولات إدارة البريد الإلكتروني (eMail
(Management Protocols

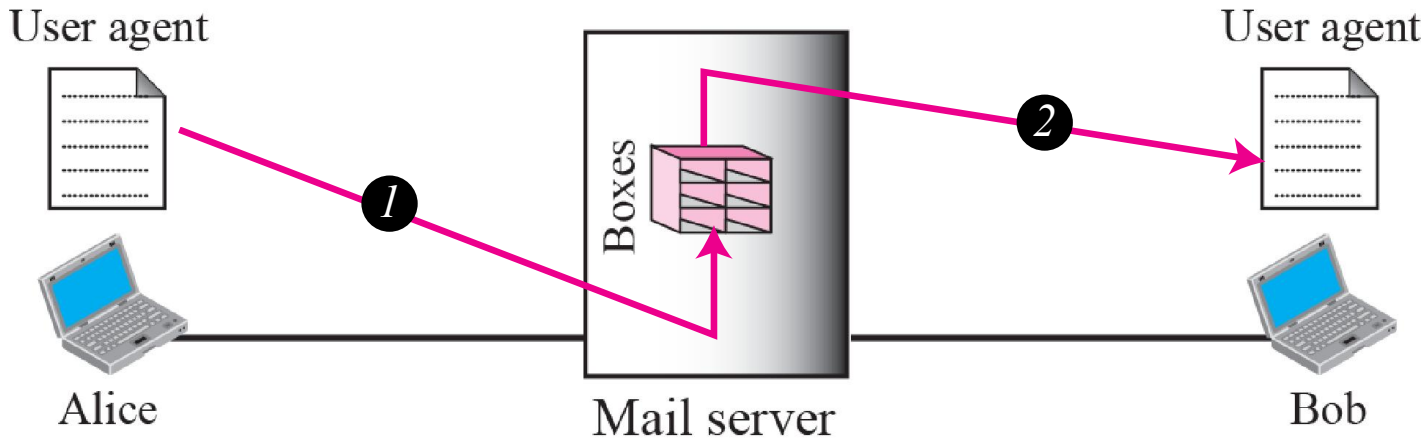
محتويات المحاضرة

- البنية (Architecture)
- عميل المستخدم (User Agent)
- عميل إرسال الرسالة (Message Transfer Agent)
- عميل النفاذ للرسالة (Message Access Agent)
- بروتوكول البريد الإلكتروني متعدد الأغراض (Multipurpose Internet Mail Extensions (MIME)

البنية (Architecture)

سيناريوهات تبادل البريد الإلكتروني

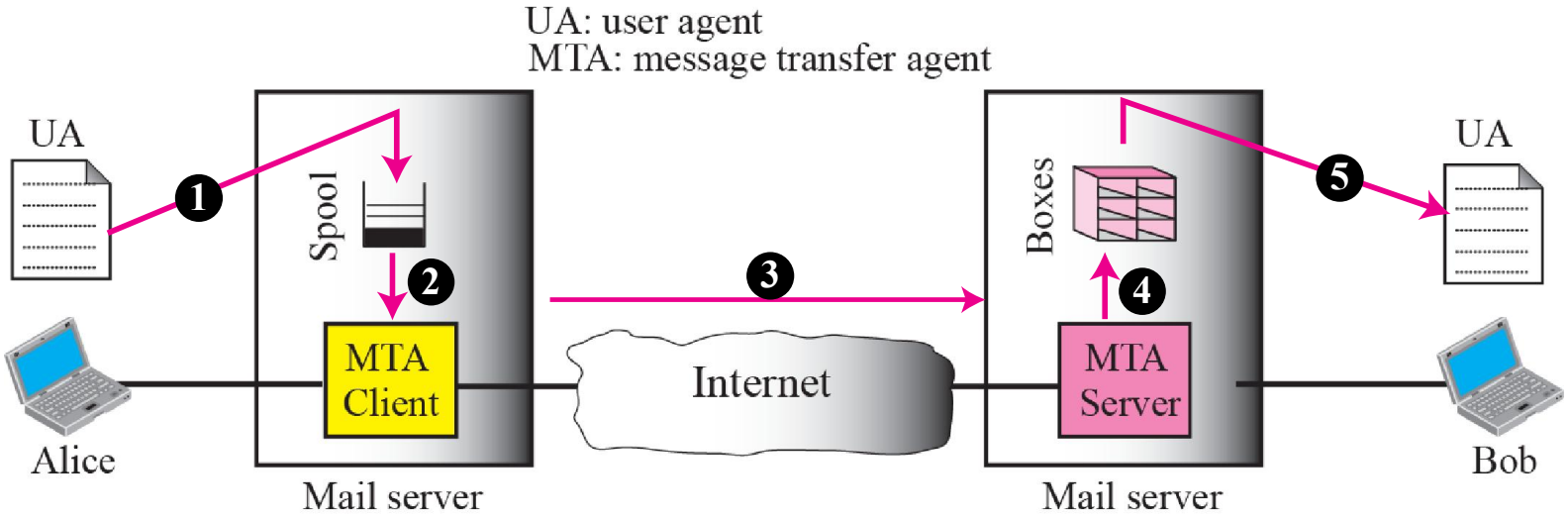
- السيناريو الأول: المرسل و المستقبل يستخدمون نفس مخدم البريد الإلكتروني (eMail Server)



Two User agents are necessary

سيناريوهات تبادل البريد الإلكتروني

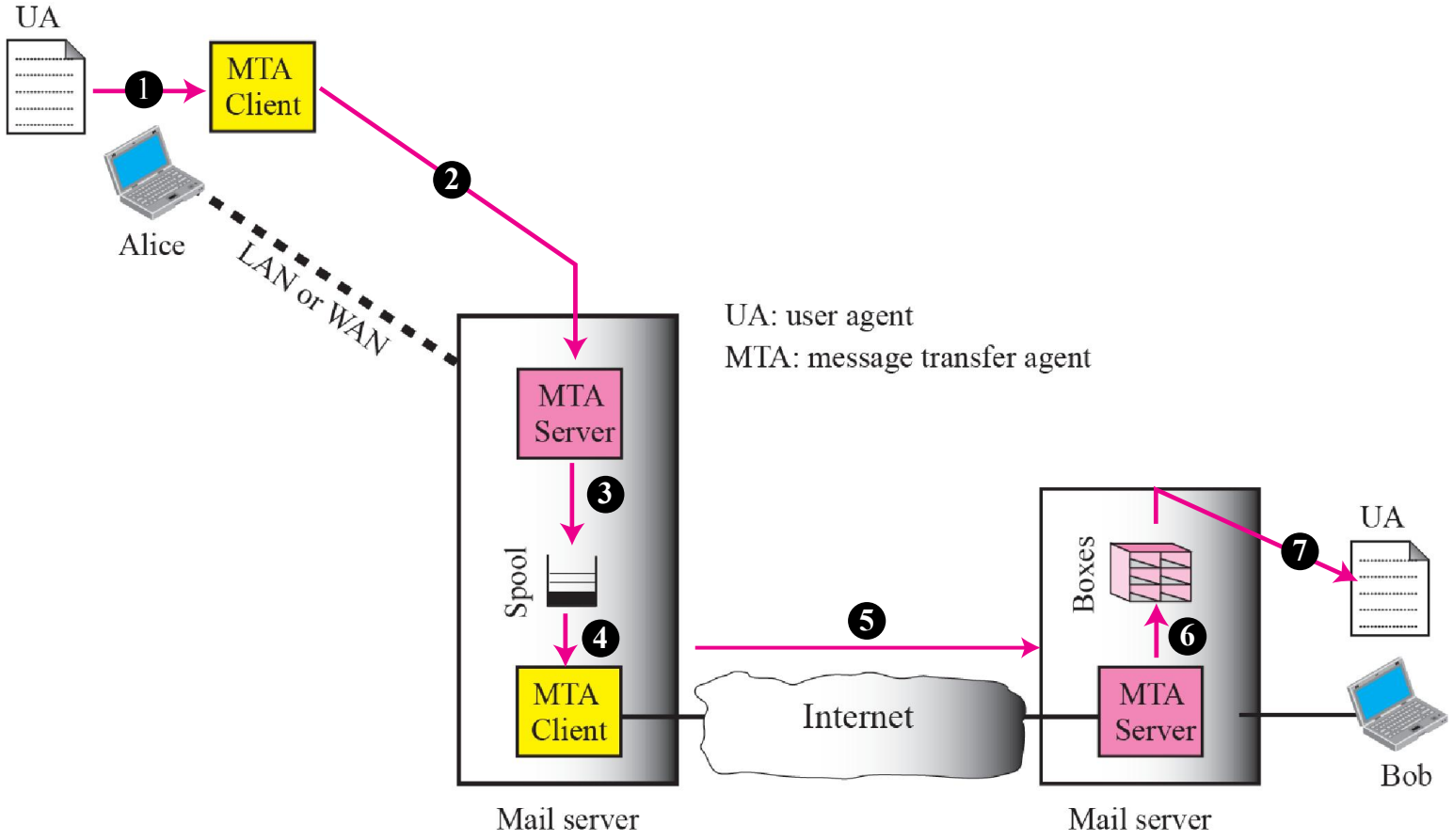
- السيناريو الثاني: المرسل و المستقبل لا يستخدمون نفس مخدم البريد الإلكتروني (eMail Server)



Two UAs and a pair of MTAs (client & server) are necessary

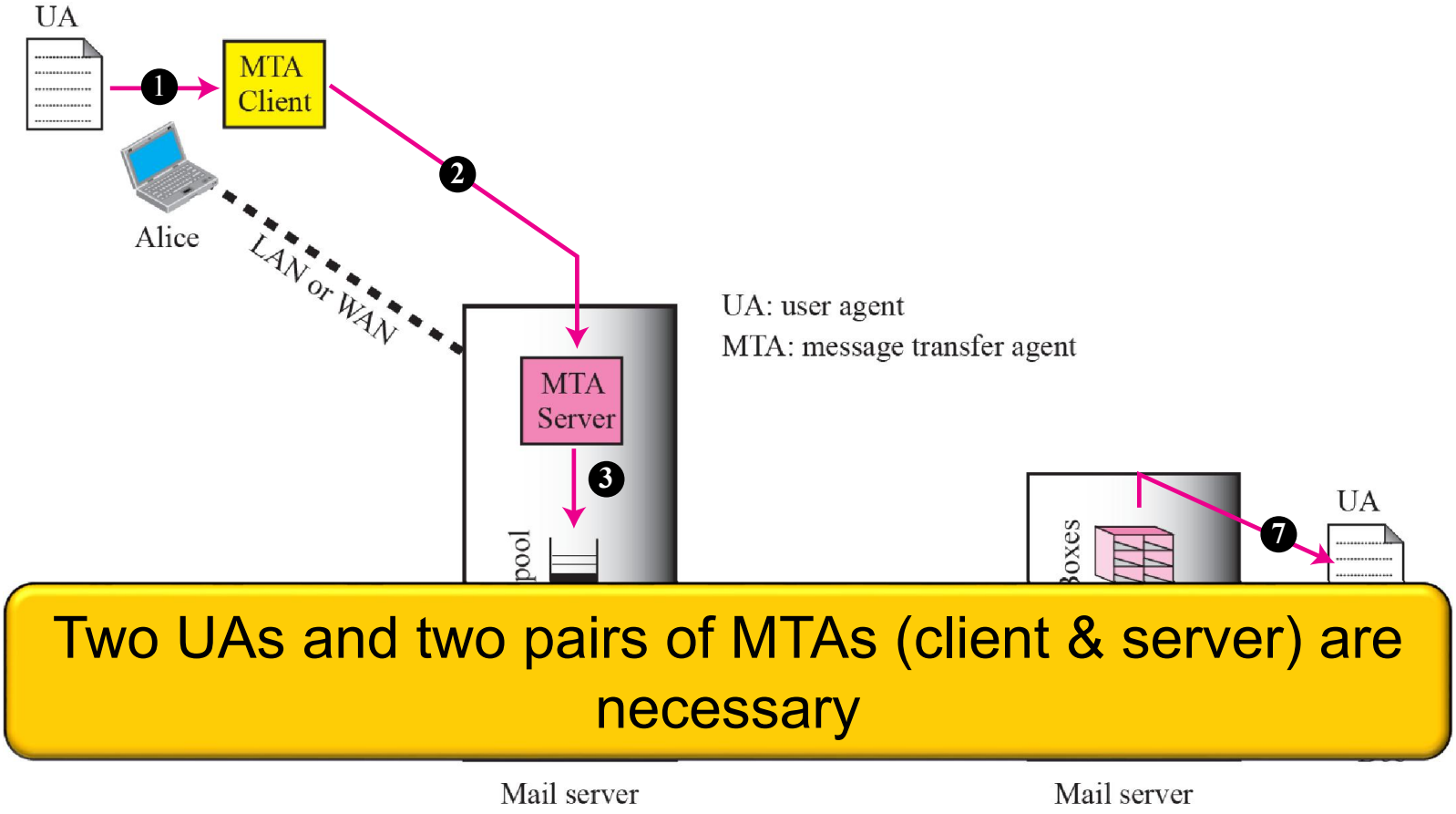
سيناريوهات تبادل البريد الإلكتروني

- السيناريو الثالث: المرسل متصل مع مخدم البريد الإلكتروني (eMail Server) باستخدام LAN أو WLAN



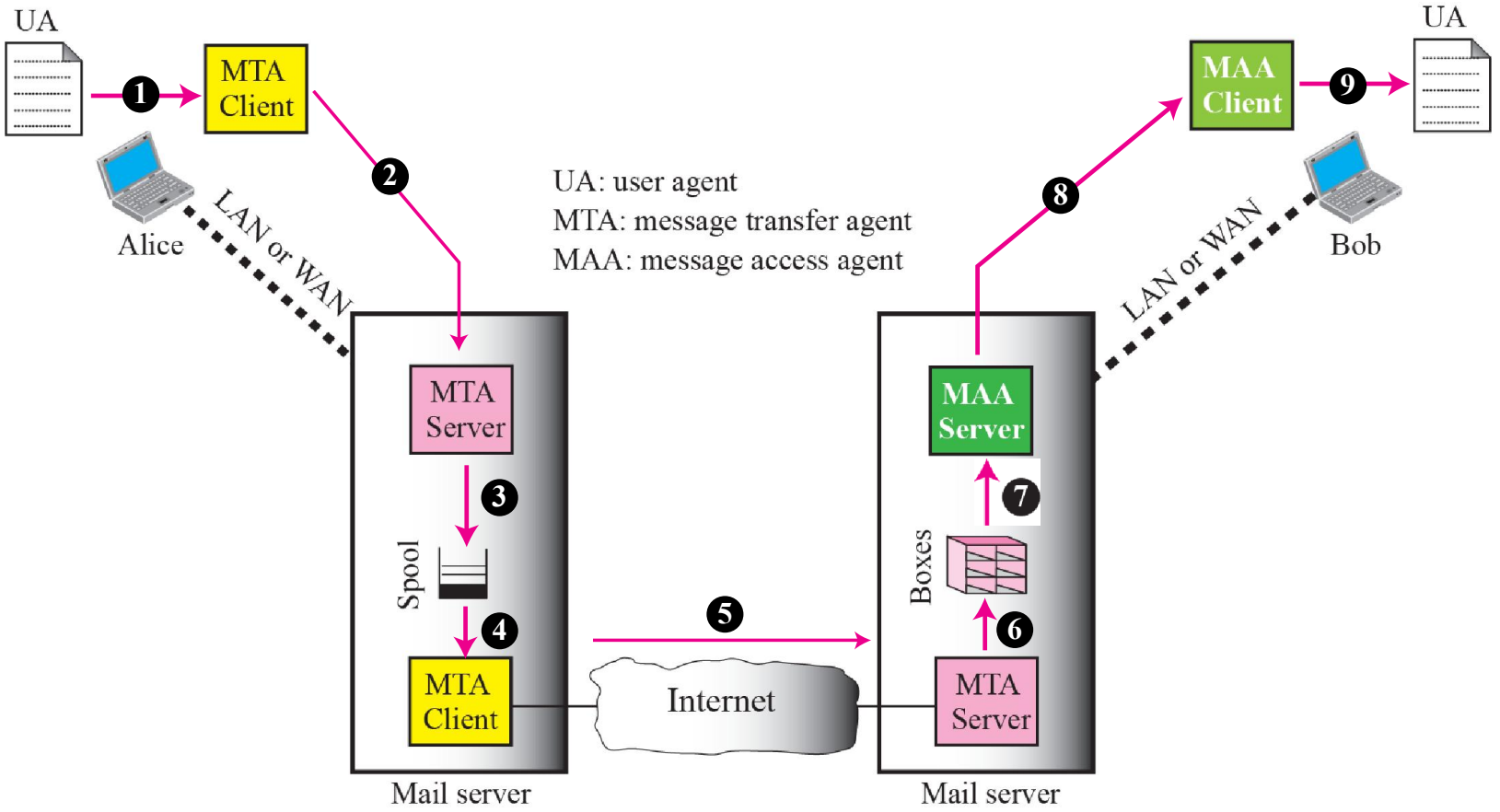
سيناريوهات تبادل البريد الإلكتروني

- السيناريو الثالث: المرسل متصل مع مخدم البريد الإلكتروني (eMail Server) باستخدام LAN أو WLAN



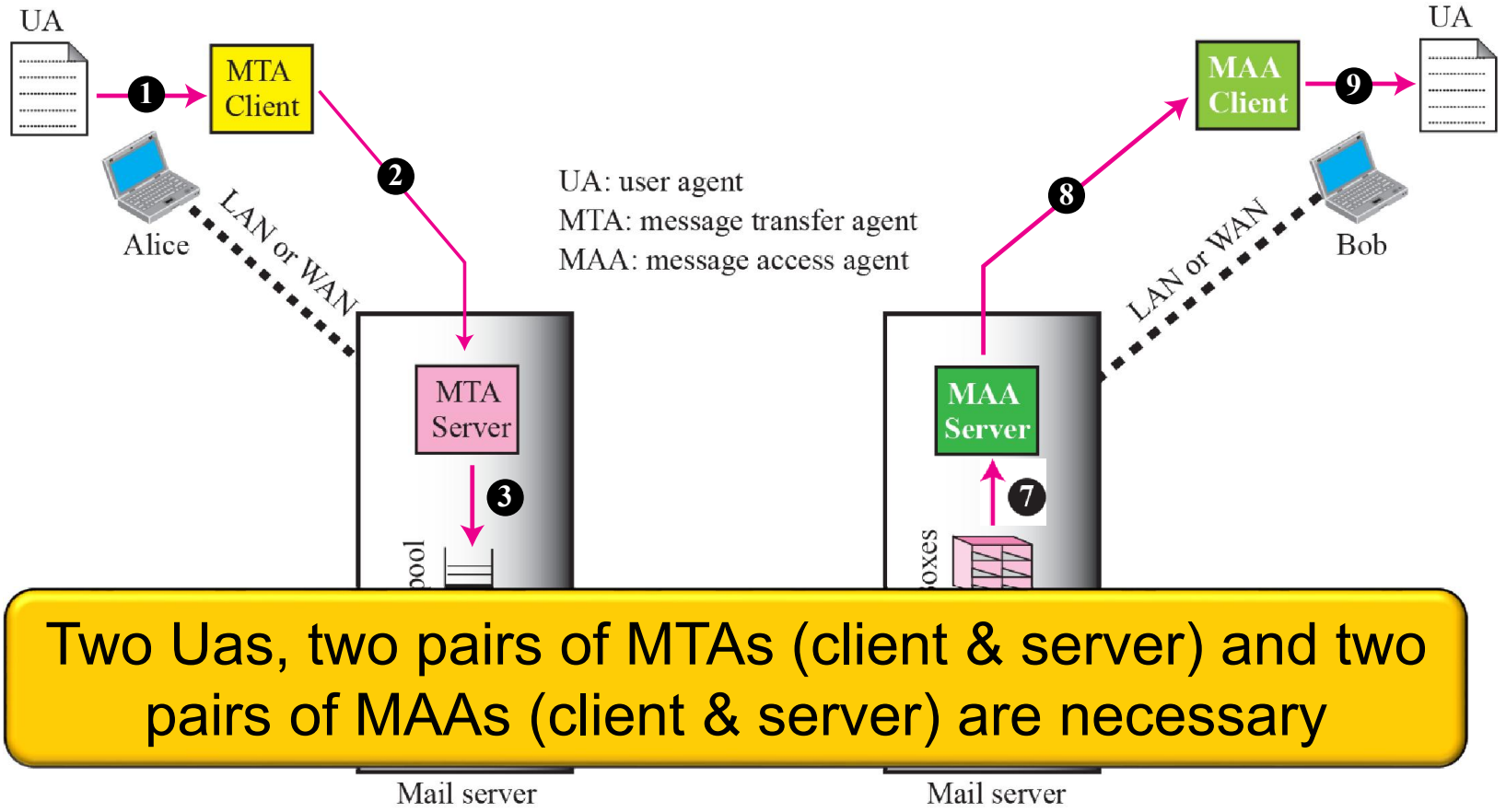
سيناريوهات تبادل البريد الإلكتروني

- السيناريو الرابع: المرسل و المستقبل متصلون مع مخدم البريد الإلكتروني (eMail Server) باستخدام LAN أو WLAN



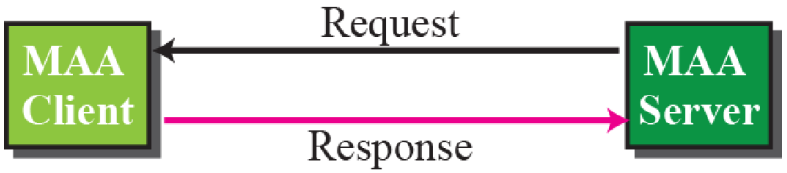
سيناريوهات تبادل البريد الإلكتروني

- السيناريو الرابع: المرسل و المستقبل متصلون مع مخدم البريد الإلكتروني (eMail Server) باستخدام LAN أو WLAN



عملية PUSH و عملية POLL

a. Client pushes messages



b. Client pulls messages

عميل المستخدم (User Agent)

ماهو عميل المستخدم (User Agent)

- UA هو المكوّن الأول من مكونات البريد الإلكتروني
- يُقدّم للمستخدم خدمة إرسال و استقبال الرسائل
- له نمطين

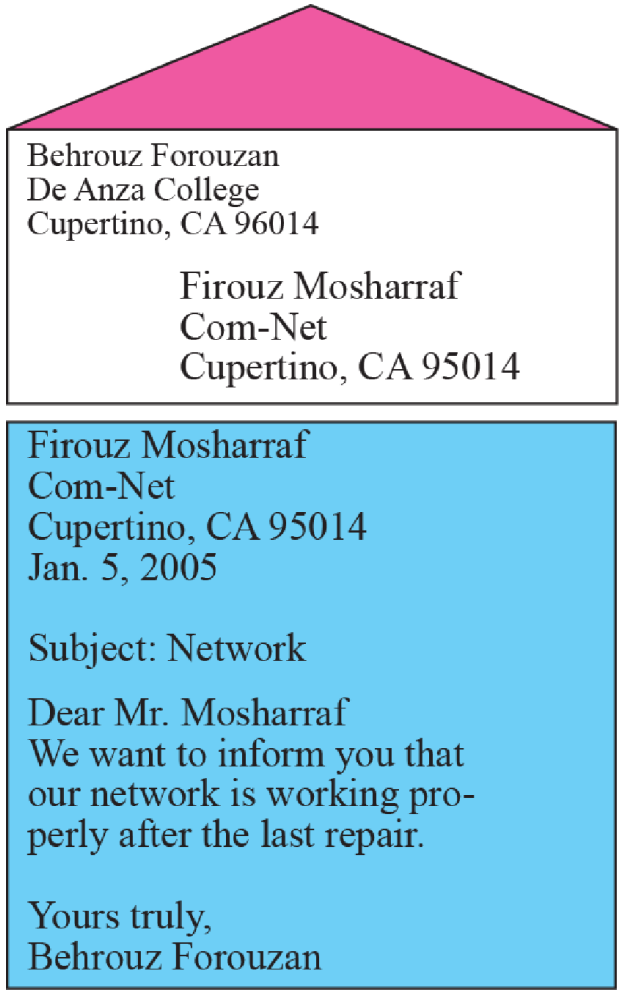
Command-driven UA –

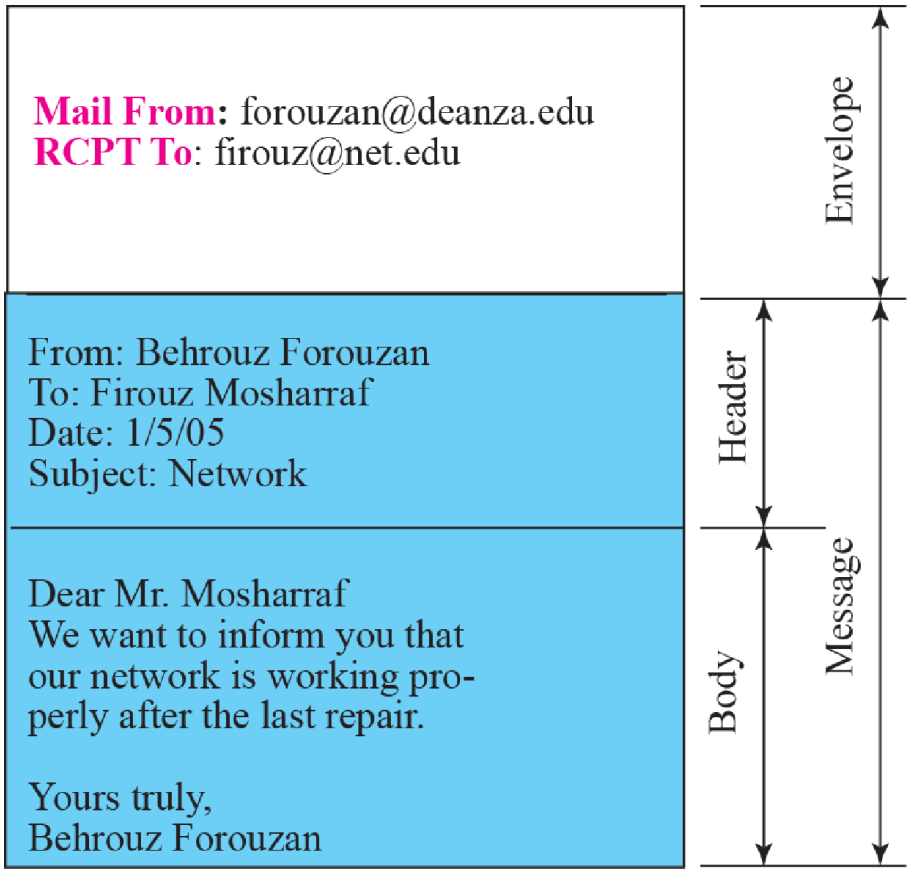
- mail, pine, elm, etc.

GUI-based UA –

- Eudora, Outlook, Netscape, etc.

صيغة الـ eMail





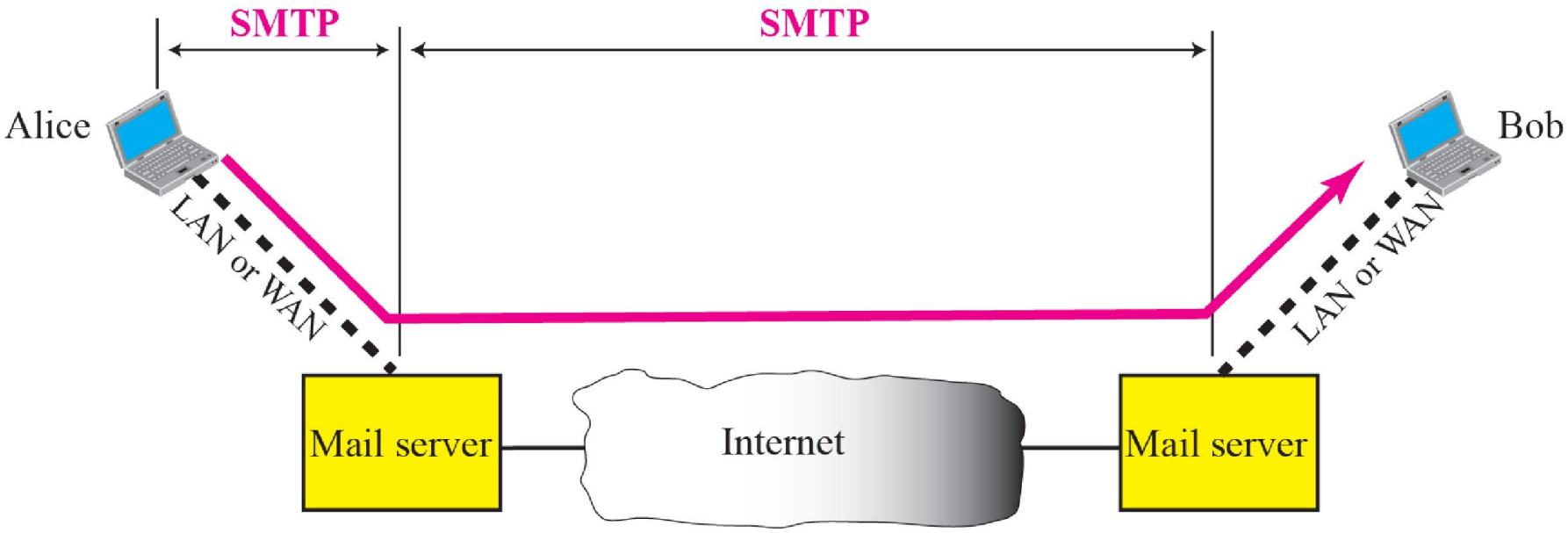
عنوان البريد الإلكتروني

عميل إرسال الرسالة (Message Transfer Agent)

ماهو عميل إرسال الرسالة (MTA)

- الإرسال الفعلي للبريد الإلكتروني يتم باستخدام عميل إرسال الرسالة (MTA)
- يجب أن يحتوي النظام على client MTA لإرسال الرسالة
- يجب أن يحتوي النظام على server MTA لاستقبال الرسالة
- البروتوكول الأساسي الذي يحدد بنية و آلية عمل الـ client MTA و الـ server MTA هو بروتوكول Simple Mail Transfer Protocol (SMTP)

مجال عمل بروتوكول SMTP



الأوامر و الإستجابة

Commands

Keyword	*Argument(s)*	*Keyword*	*Argument(s)*
HELO	Sender's host name	NOOP	
MAIL FROM	Sender of the message	TURN	
RCPT TO	Intended recipient	EXPN	Mailing list
DATA	Body of the mail	HELP	Command name
QUIT		SEND FROM	Intended recipient
RSET		SMOL FROM	Intended recipient
VRFY	Name of recipient	SMAL FROM	Intended recipient

الأوامر و الإستجابة

Responses

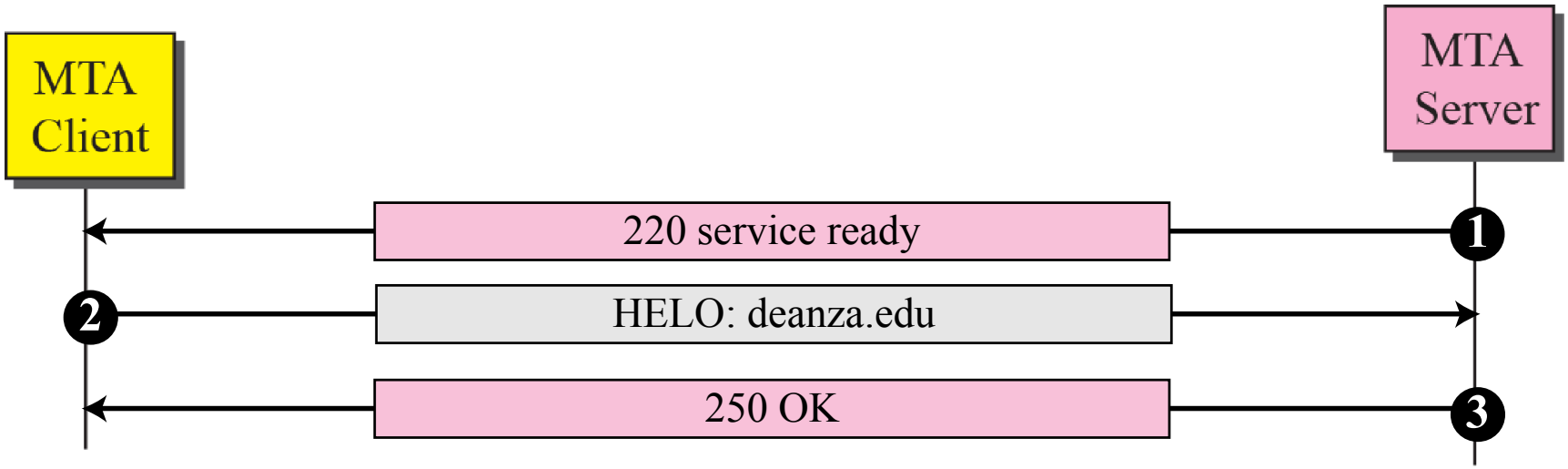
Code	*Description*
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage

الأوامر و الإستجابة

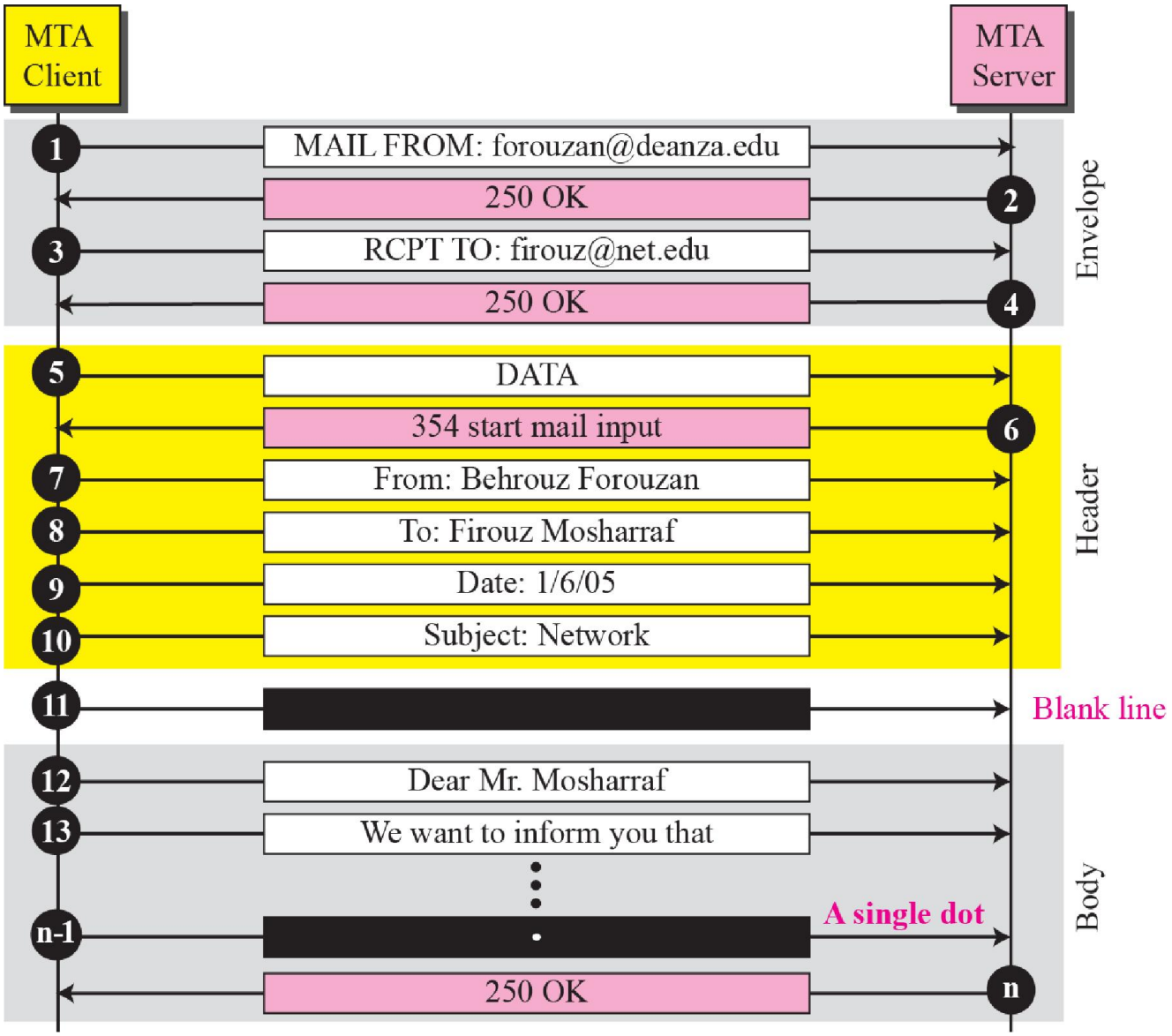
Responses

Permanent Negative Completion Reply	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

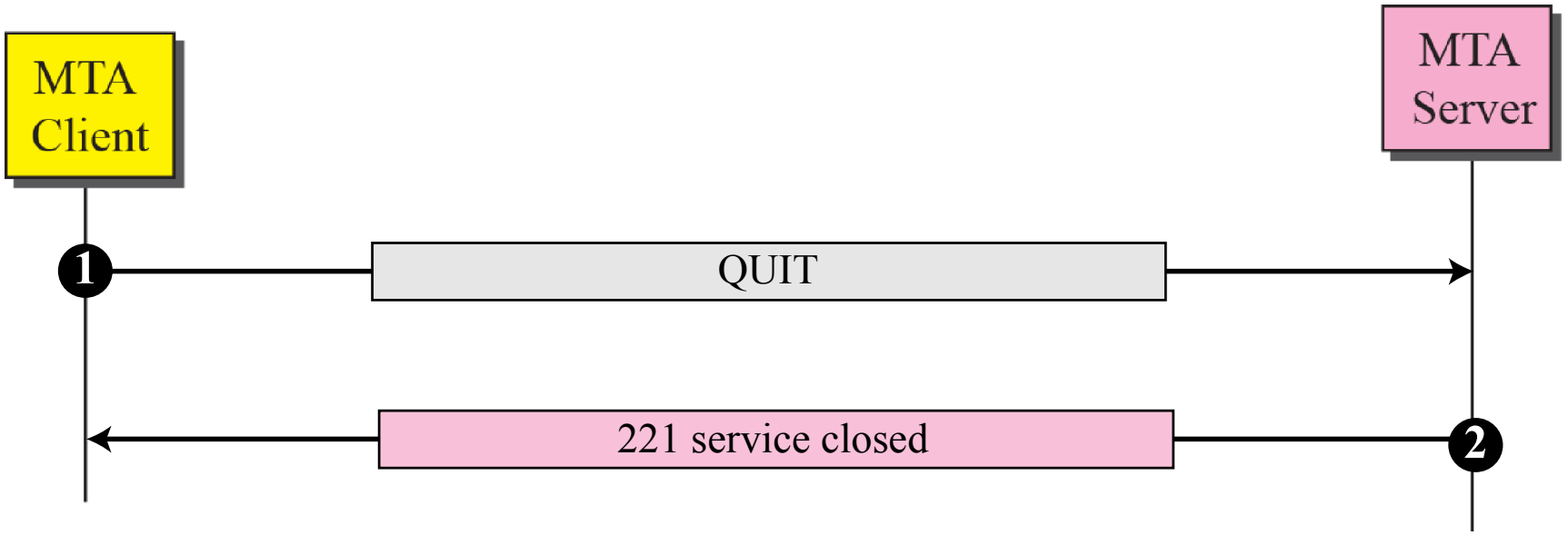
تأسيس الوصلة (Connection establishment)



نقل الرسالة (Message transfer)



(Connection termination) إنهاء الوصلة



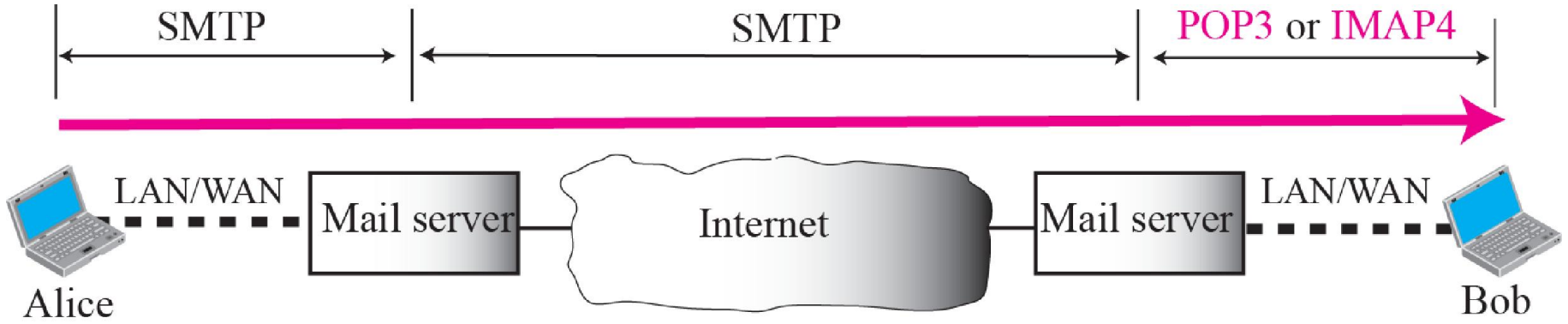
عميل النفاذ للرسالة (Message Access Agent)

لماذا نحتاج عميل النفاذ للرسالة (Message Access Agent)

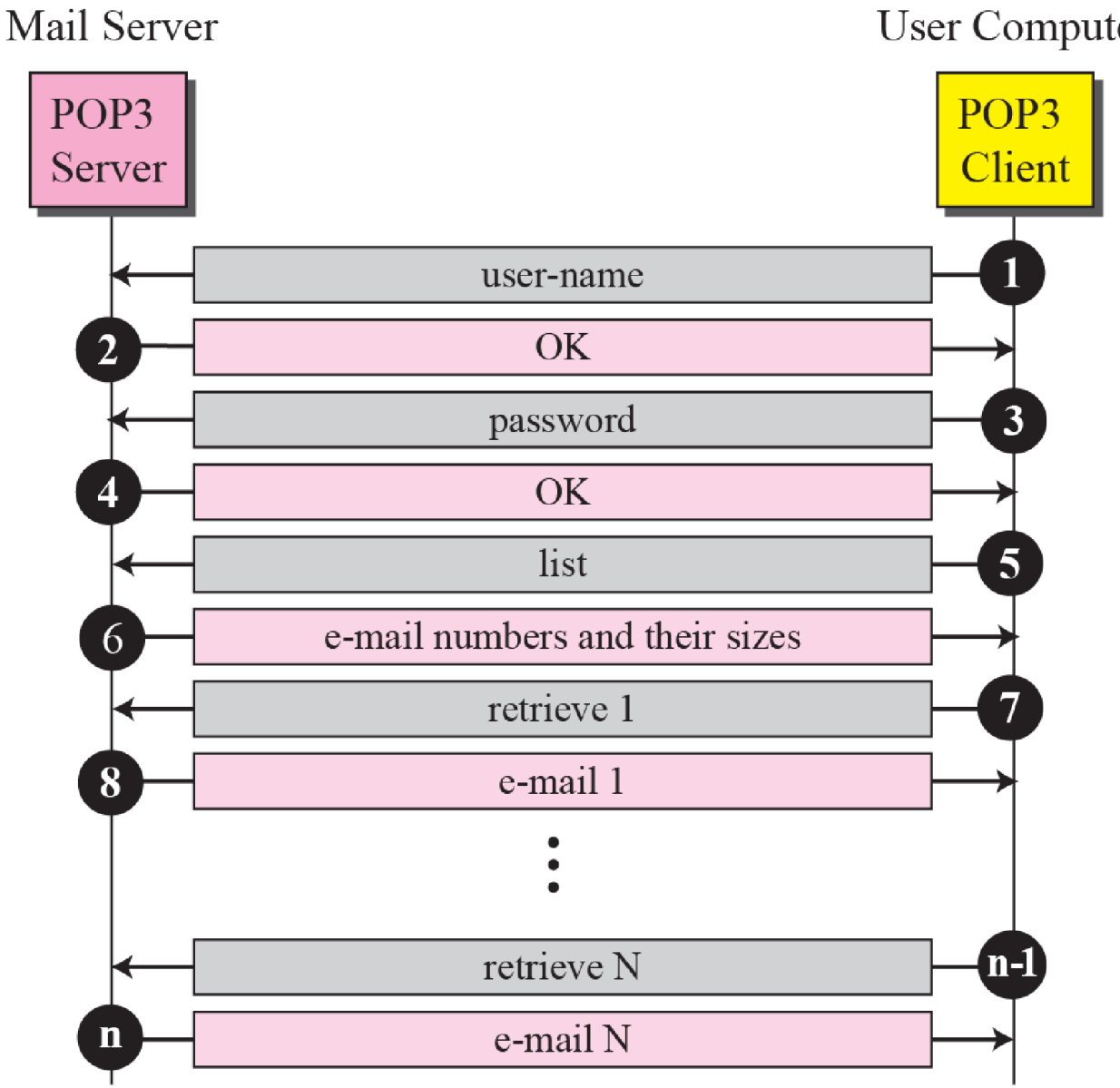
- SMTP
  - a push protocol
  - يرسل رسائل البريد الإلكتروني من الزبون إلى المخدم (pushes the message from the client to the server)

- لجلب الرسائل من المخدم إلى الزبون نحتاج إلى بروتوكول
  - The direction of the bulk data are from the server to the client
  - نحتاج لعميل النفاذ للرسالة (Message Access Agent (MAA))
  - أمثلة
    - POP3
    - IMAP4

Pop3 و IMAP4


SMTP
SMTP
POP3 or IMAP4
LAN/WAN
Mail server
Internet
Mail server
LAN/WAN
Alice
Bob

Pop3


Mail Server
User Computer
POP3 Server
POP3 Client
user-name
1
2
OK
password
3
4
OK
list
5
6
e-mail numbers and their sizes
retrieve 1
7
8
e-mail 1
retrieve N
n-1
n
e-mail N

بروتوكول البريد الإلكتروني متعدد الأغراض
Multipurpose Internet Mail Extensions)
((MIME)

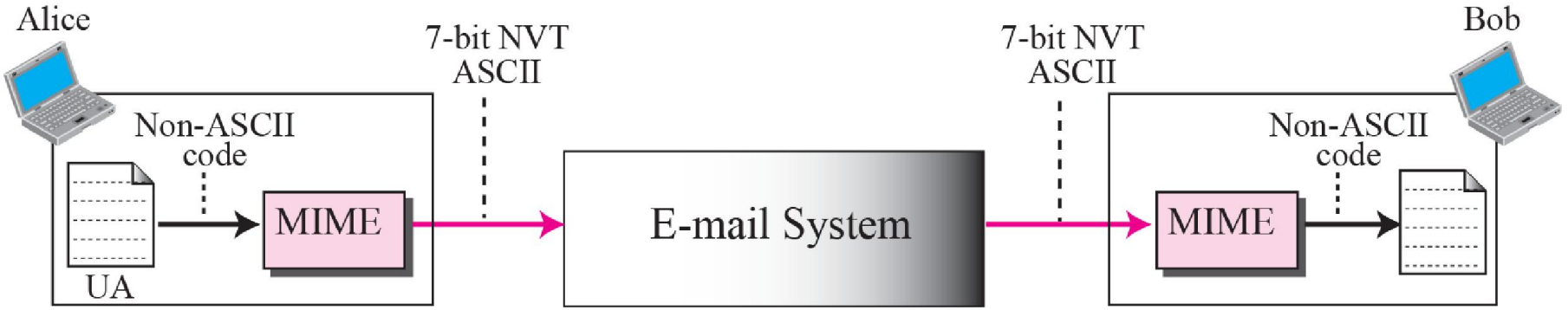
وظيفة بروتوكول MIME

- إرسال البريد الإلكتروني عملية سهلة, لكن هذا على حساب الصيغة التي يتم فيها إرسال البريد الإلكتروني
  - يتم إرسال الرسالة بتنسيق NVT 7-bit ASCII

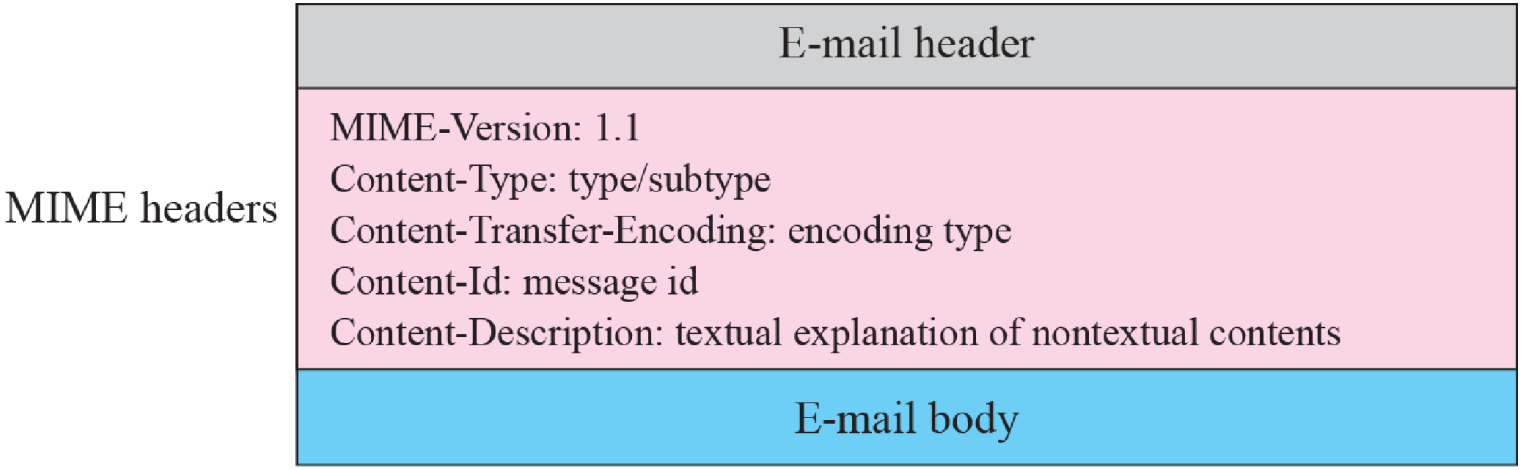
- بروتوكول MIME هو بروتوكول مكمل (supplementary protocol), حيث يسمح بإرسال non-ASCII data عبر البريد الإلكتروني

- يقوم بروتوكول MIME بـ
  - تحويل non-ASCII data في جهة المرسل إلى NVT ASCII data
  - يرسل البيانات إلى MTA, الذي بدوره يرسلها عبر البريد الإلكتروني
  - يتم تحويل الرسالة المستقبلة مجدداً إلى الصيغة الأصلية

وظيفة بروتوكول MIME



ترويسة بروتوكول MIME



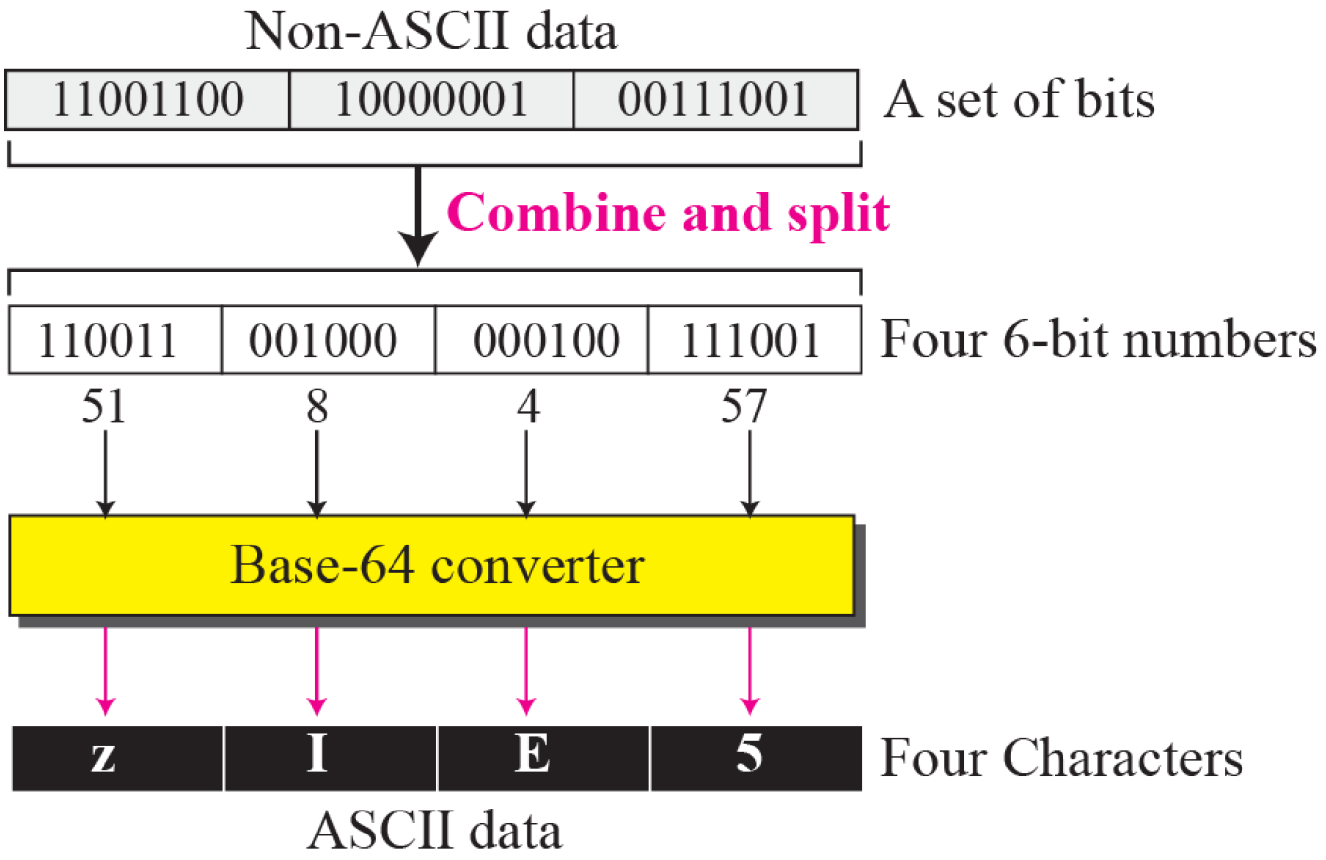
أنماط المعطيات في بروتوكول MIME

Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format (see Appendix E)
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to Mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 KHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (eight-bit bytes)

أنماط المعطيات في بروتوكول MIME (Content transfer encoding)

Type	*Description*
7bit	NVT ASCII characters and short lines
8bit	Non-ASCII characters and short lines
Binary	Non-ASCII characters with unlimited-length lines
Base64	6-bit blocks of data are encoded into 8-bit ASCII characters
Quoted-printable	Non-ASCII characters are encoded as an equal sign plus an ASCII code

أنماط المعطيات في بروتوكول MIME (Base64)

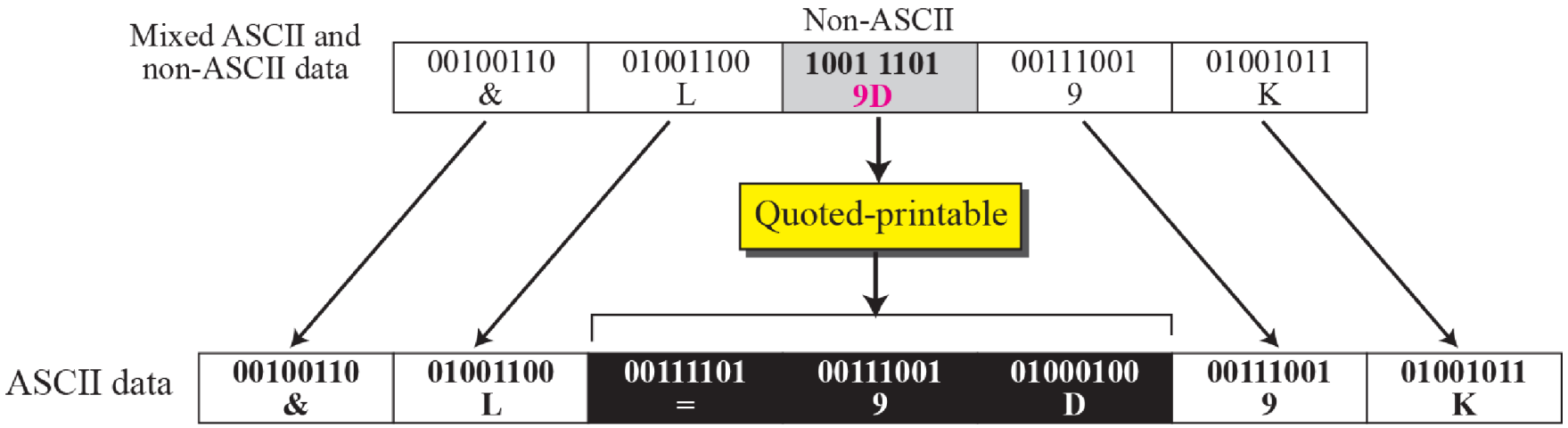


أنماط المعطيات في بروتوكول MIME (Base64)

- Base 64 converting table

Value	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*	*Value*	*Code*
0	**A**	11	**L**	22	**W**	33	**h**	44	**s**	55	**3**
1	**B**	12	**M**	23	**X**	34	**i**	45	**t**	56	**4**
2	**C**	13	**N**	24	**Y**	35	**j**	46	**u**	57	**5**
3	**D**	14	**O**	25	**Z**	36	**k**	47	**v**	58	**6**
4	**E**	15	**P**	26	**a**	37	**l**	48	**w**	59	**7**
5	**F**	16	**Q**	27	**b**	38	**m**	49	**x**	60	**8**
6	**G**	17	**R**	28	**c**	39	**n**	50	**y**	61	**9**
7	**H**	18	**S**	29	**d**	40	**o**	51	**z**	62	+
8	**I**	19	**T**	30	**e**	41	**p**	52	**0**	63	/
9	**J**	20	**U**	31	**f**	42	**q**	53	**1**		
10	**K**	21	**V**	32	**g**	43	**r**	54	**2**		

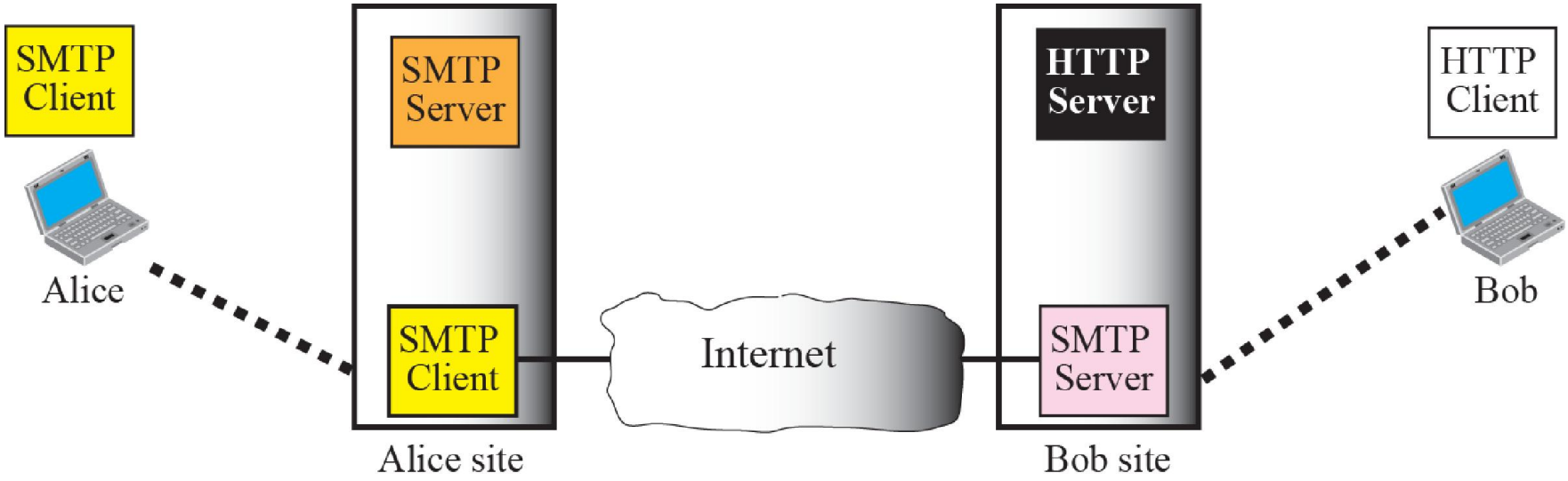
أنماط المعطيات في بروتوكول MIME (Quoted printable)



Web-Based e-MAIL

- يتم استخدام مواقع إنترنت لإرسال البريد الإلكتروني (Hotmail, Yahoo, Google, etc.)

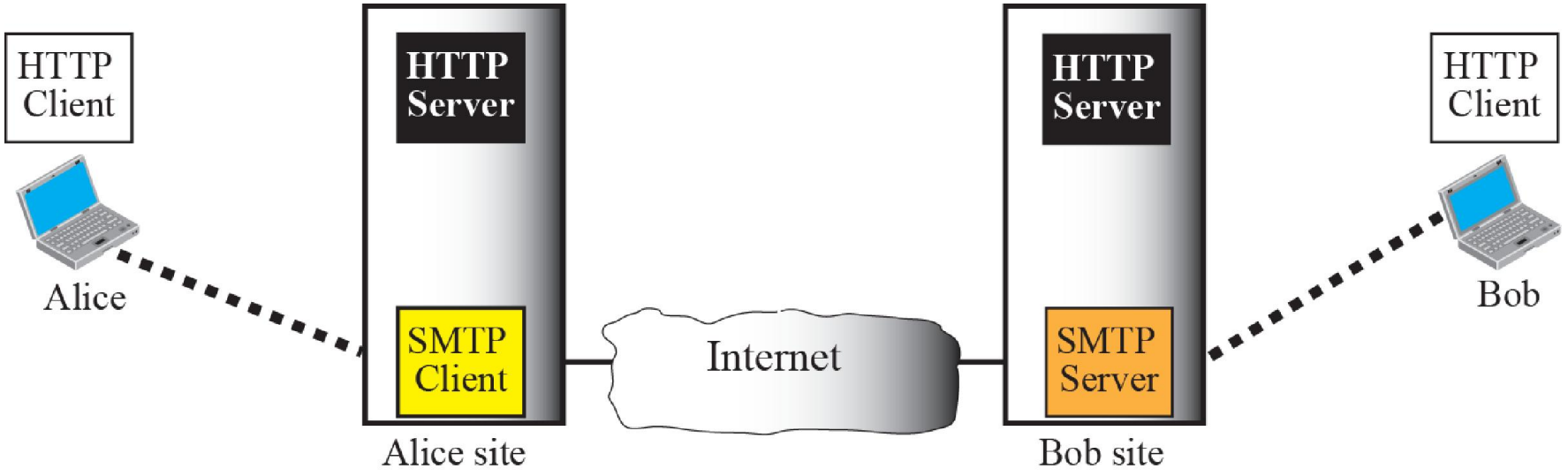
- الحالة 1



Web-Based e-MAIL

- يتم استخدام مواقع إنترنت لإرسال البريد الإلكتروني (Hotmail, Yahoo, Google, etc.)

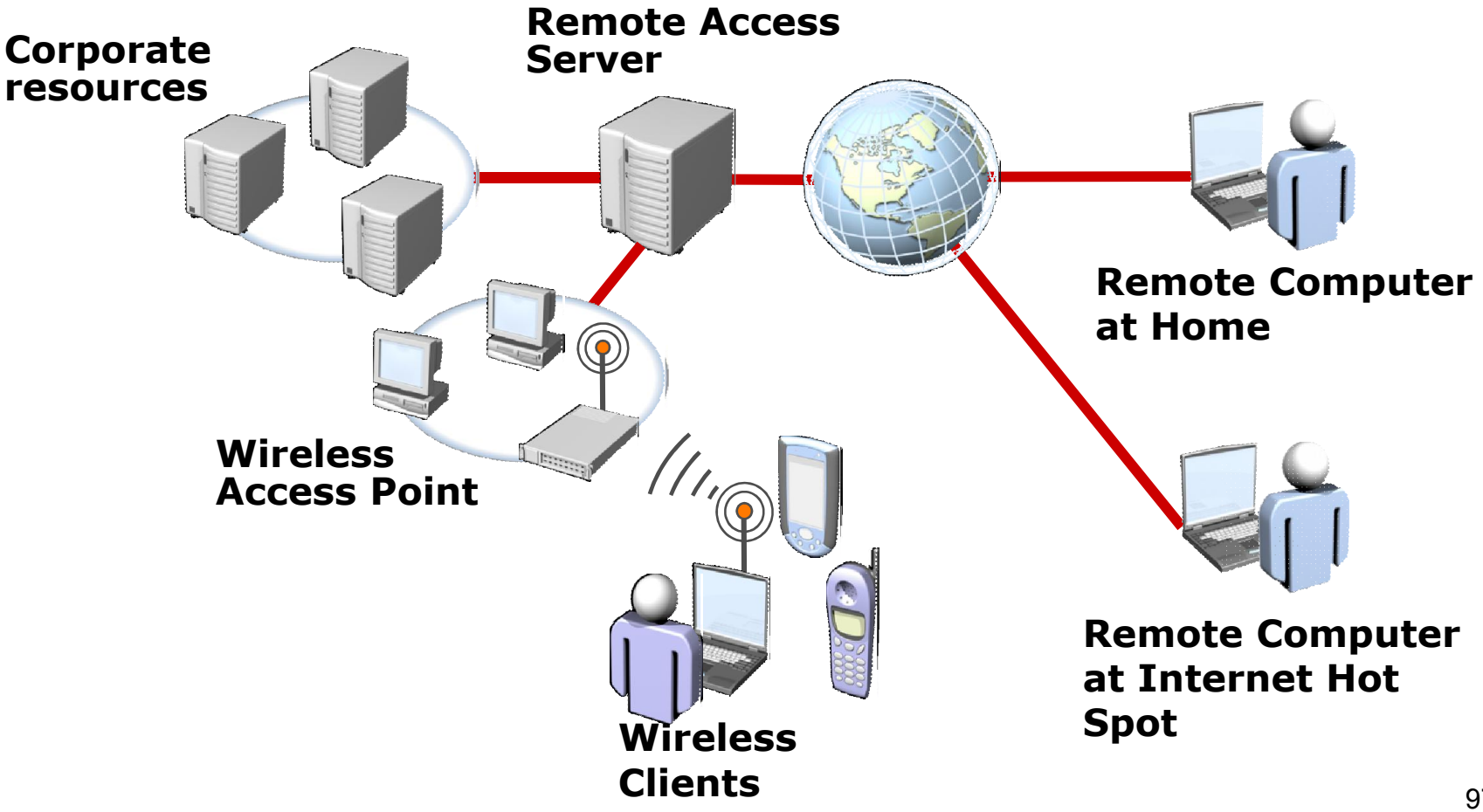
- الحالة 2



النفاذ عن بعد (Remote access)

ماهو النفاذ عن بعد (Remote access)

- النفاذ عن بعد: هو النفاذ لمجموعة من المصادر المشتركة (corporate resources) من خارج الشبكة (corporate network)



بروتوكولات VPN

- تستخدم وصلات VPN العديد من البروتوكولات لتأمين التشفير و الحماية

VPN Protocol	Description
Point-to-Point Tunneling Protocol (PPTP)	• Widely supported in clients • Traverses NAT easily • Easy to configure
Layer 2 Tunneling Protocol (L2TP)	• Uses IPsec to encrypt data • Increased security over PPTP • More difficult to configure
Secure Socket Tunneling Protocol (SSTP)	• Uses Secure Sockets Layer (SSL) to encrypt data • Can pass through proxy servers on port 443 • Easy to configure