

Protocols and Port Numbers



Ross Bagurdes

NETWORK ENGINEER

@bagurdes



Module Goals



Application Layer Protocols

- Data Transfer Protocols
- Authentication Protocols
- Network Service Protocols
- Network Management Protocols
- Audio/Visual Protocols

OSI Model

7	Application Layer
6	Presentation Layer
5	Session Layer
4	Transport Layer
3	Network Layer
2	Data Link Layer
1	Physical Layer

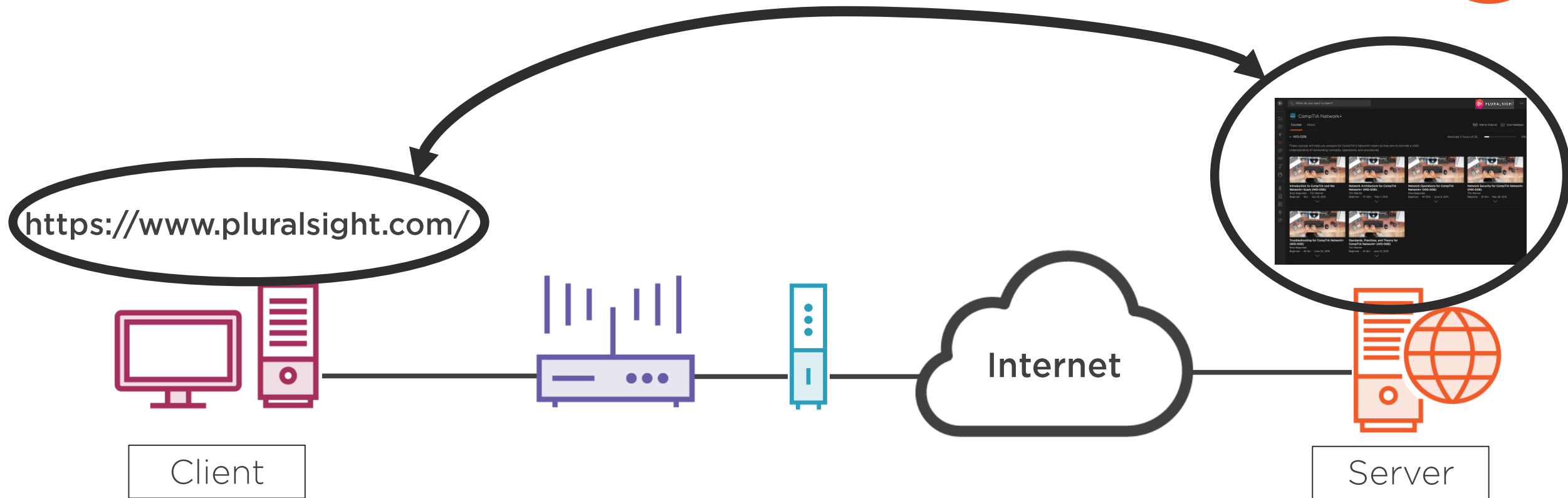


Application Layer Protocols



Transferring Data

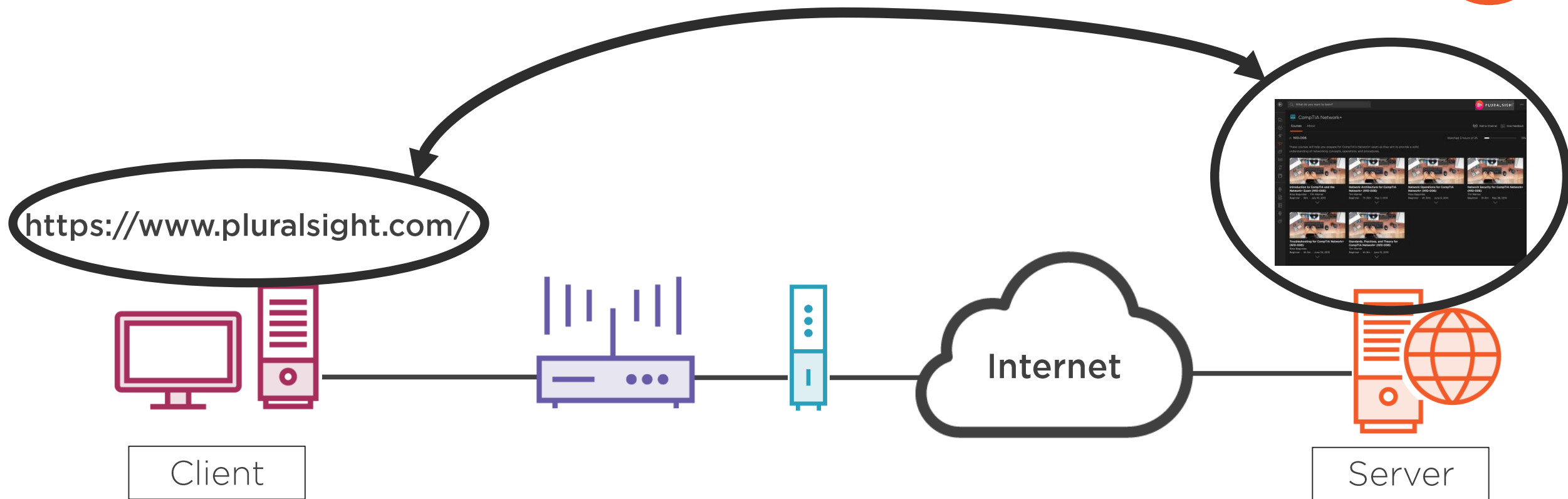




Application Layer Protocols



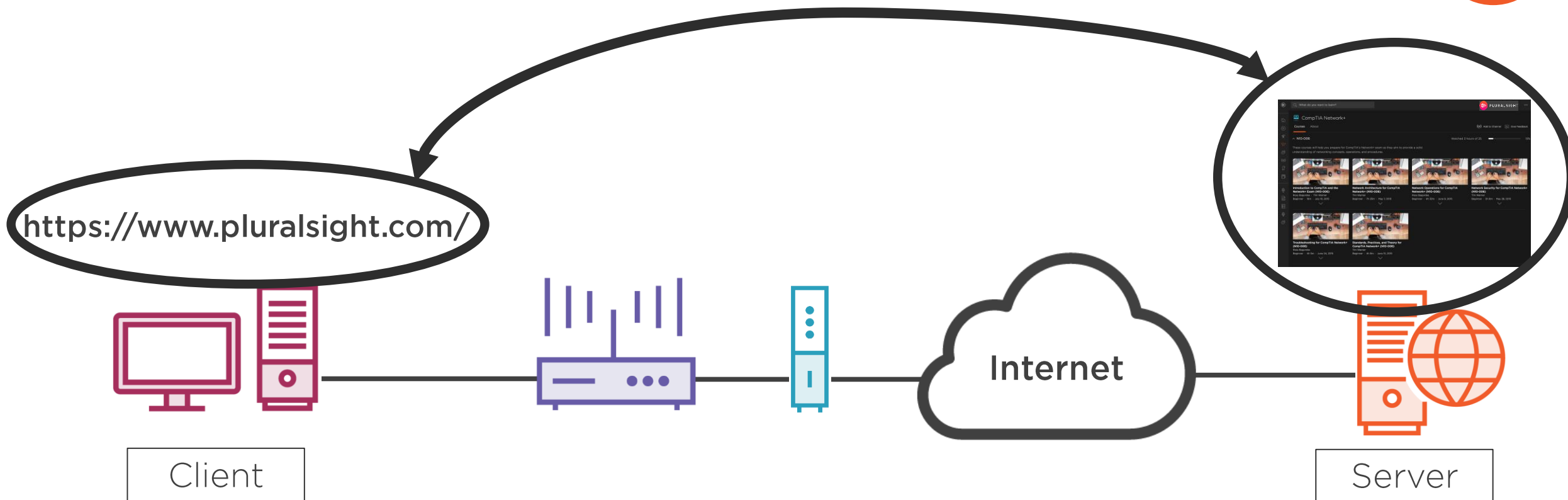
1.1



HTTP HTTPS



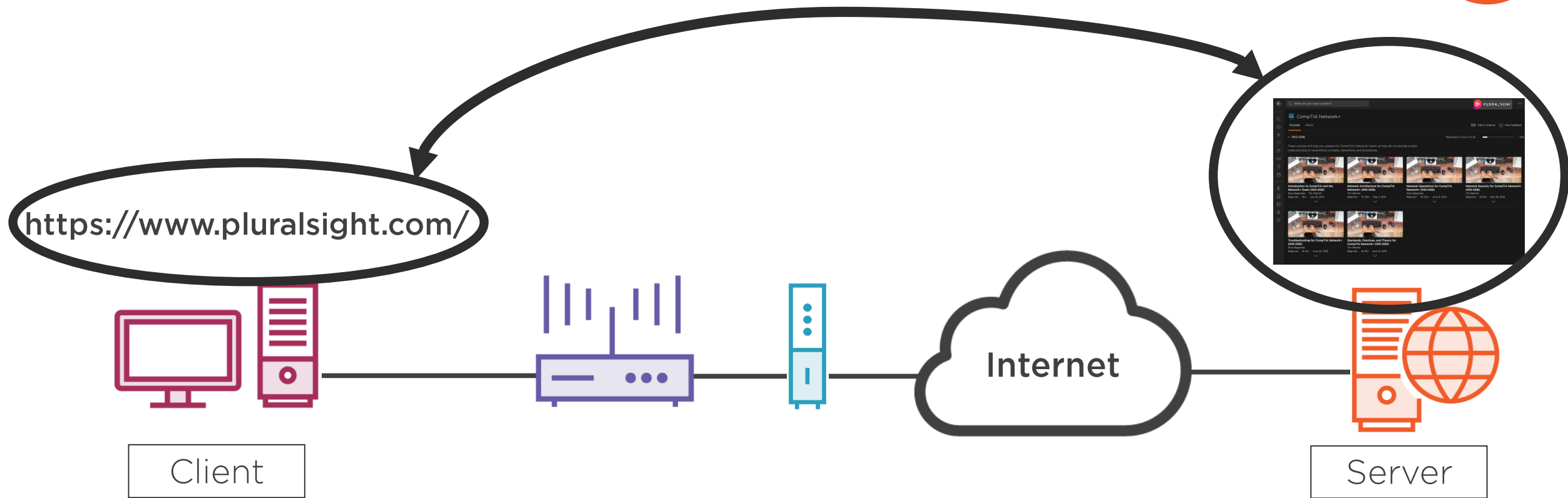
1.1



HTTP HTTPS

Hypertext Transfer Protocol (secure)

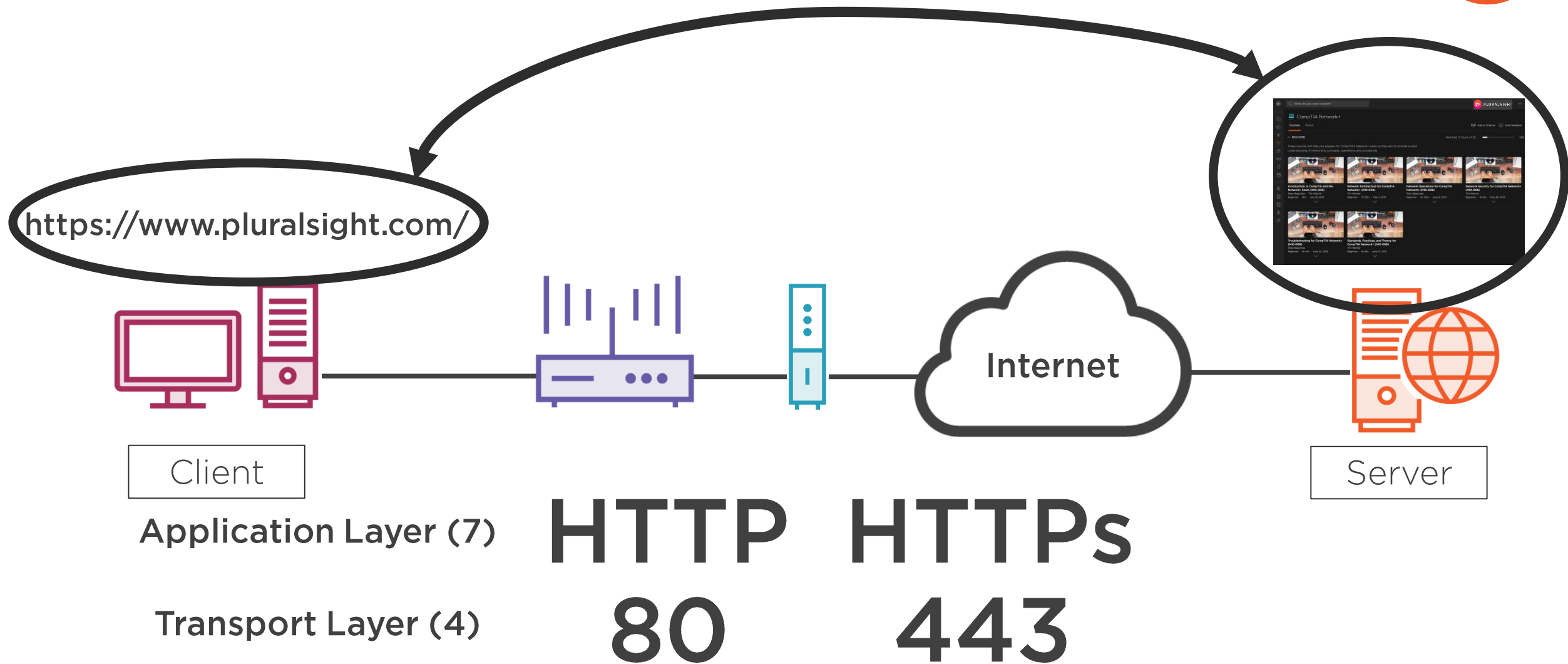




Application Layer (7)

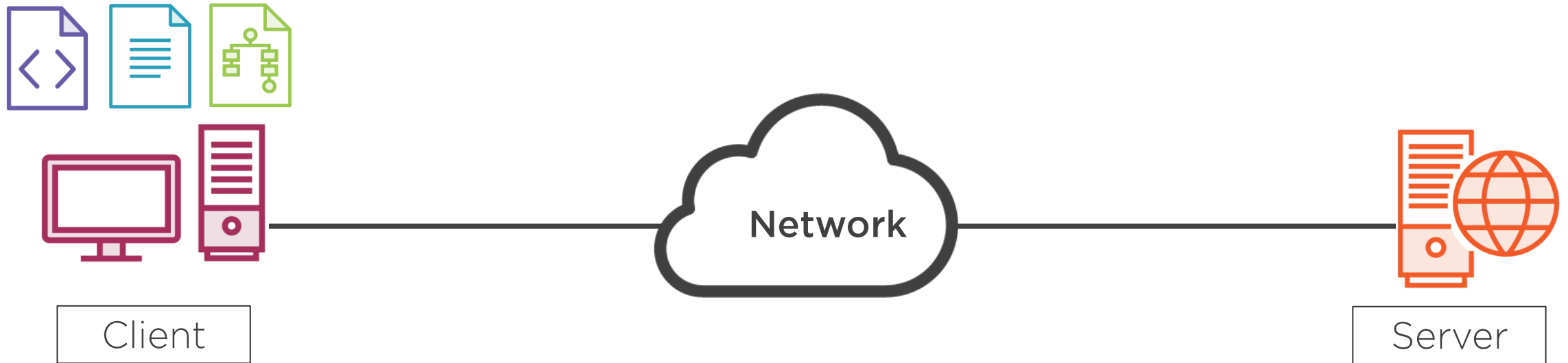
HTTP HTTPS







File Transfer

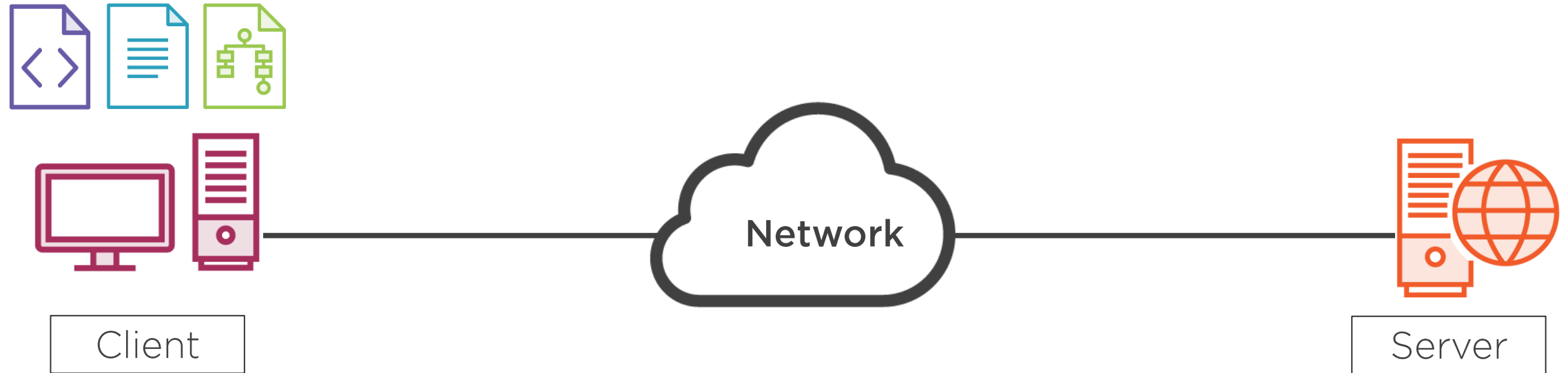


File Transfer



File Transfer





File Transfer



File Transfer

FTP SFTP TFTP



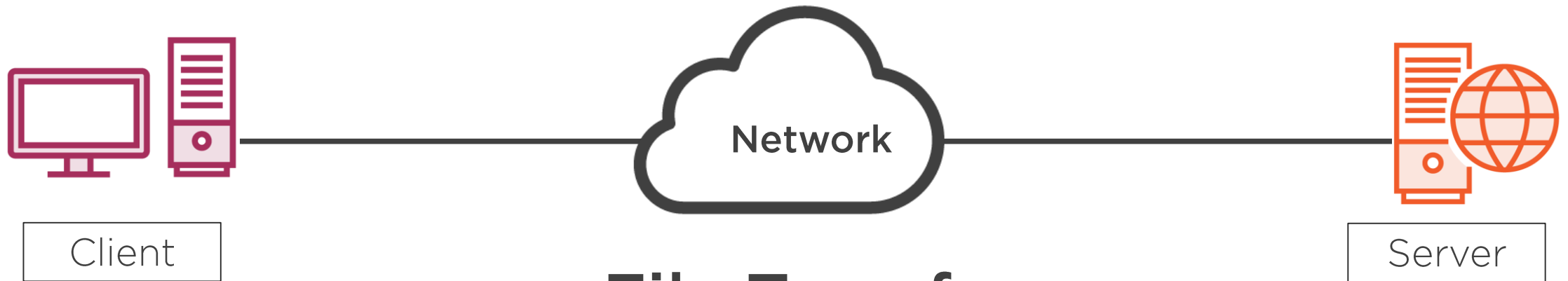
File Transfer

FTP
20 21

sFTP
22

TFTP
69





File Transfer

FTP	sFTP	TFTP	SMB
20	21	22	69
			445

Demonstration:

Examine FTP and SMB operation





Email





Client

Network

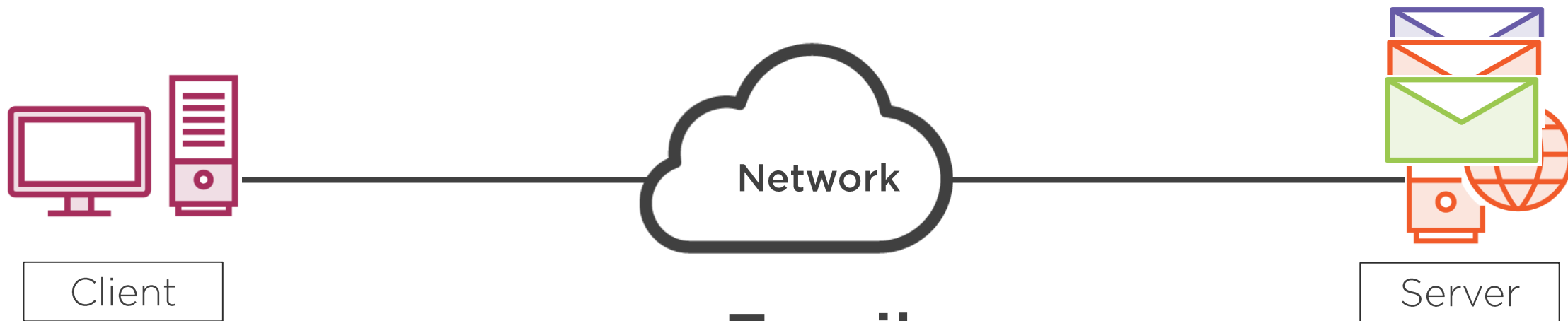
Server

Email

POP3

IMAP

SMTP



POP3 IMAP





SMTP



Email

SMTP



Email

SMTP



Email

SMTP





Email

POP3
110/995

IMAP
143/993

SMTP
25/465



Demonstration:

Examine POP3, IMAP, and SMTP



Authentication





Authentication



LDAP

LDAPs



Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol





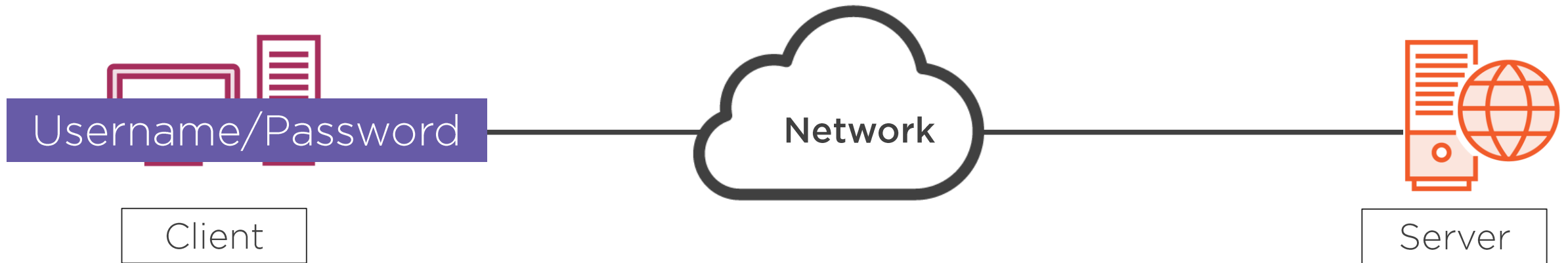
Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol





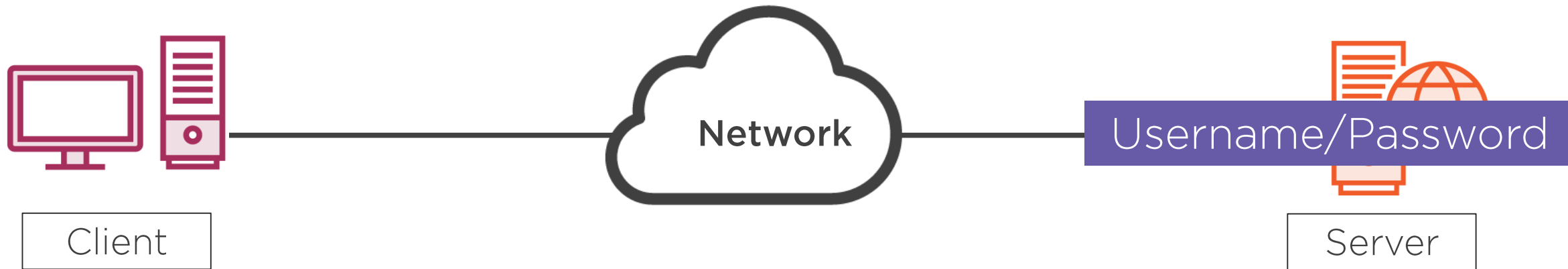
Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol





Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol





Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol



Authentication

LDAP

LDAPs

Lightweight Directory Access Protocol



Authentication

LDAP
389

LDAPs
636

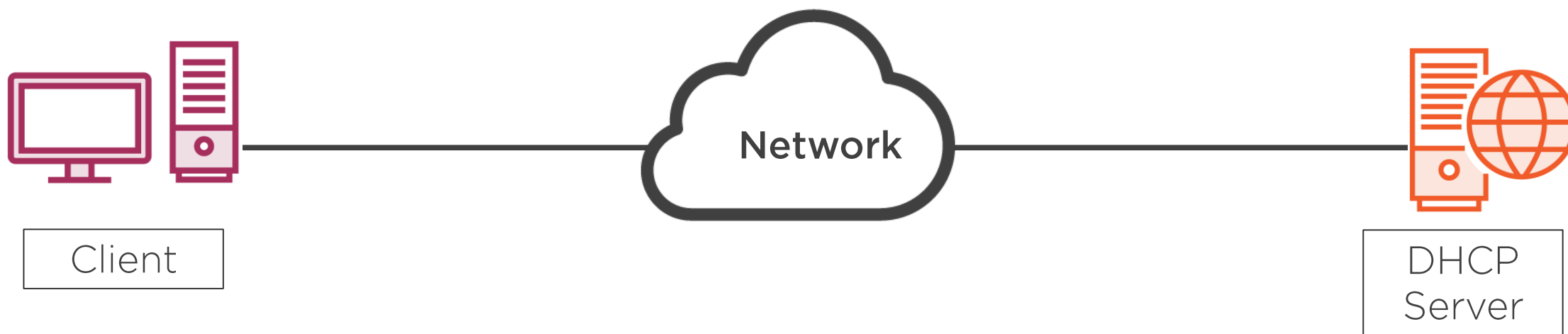
Network Services





Dynamic Host Configuration Protocol





DHCP





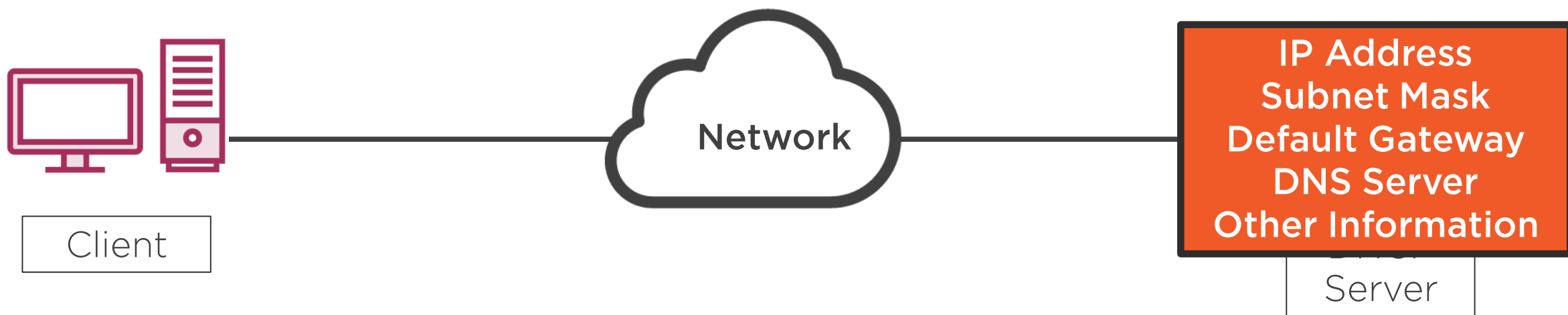
DHCP





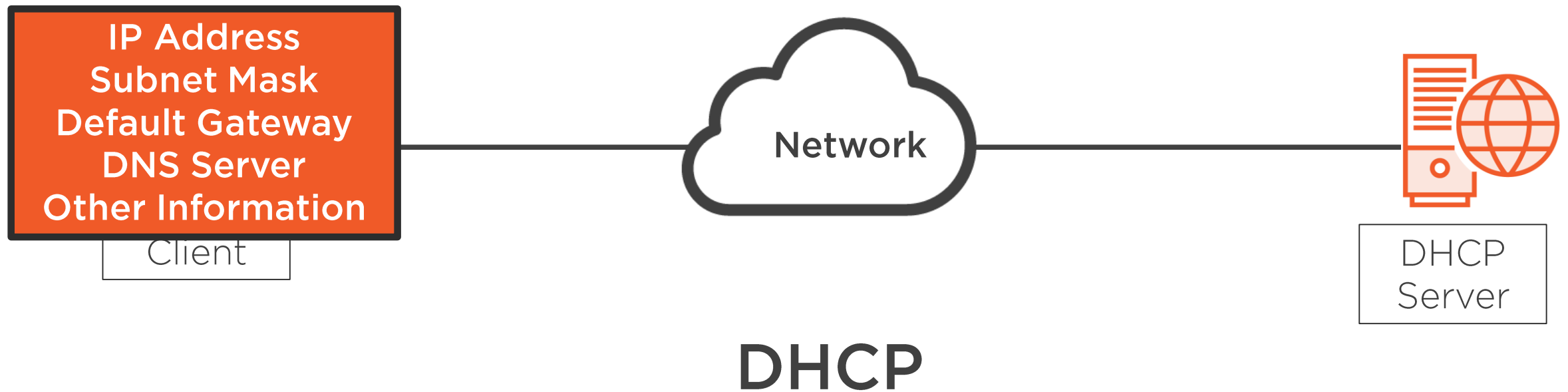
DHCP





DHCP





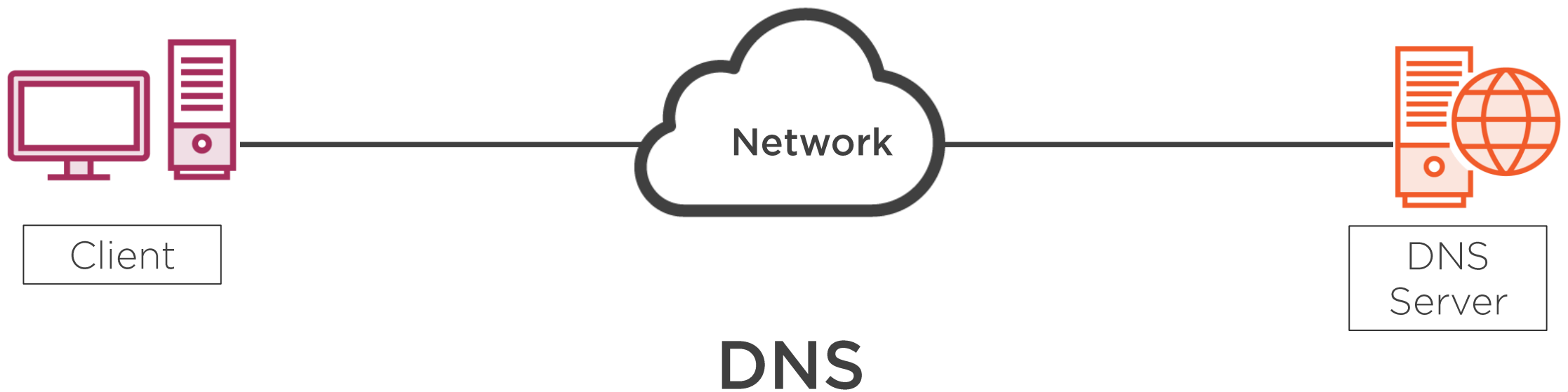
Demonstration:

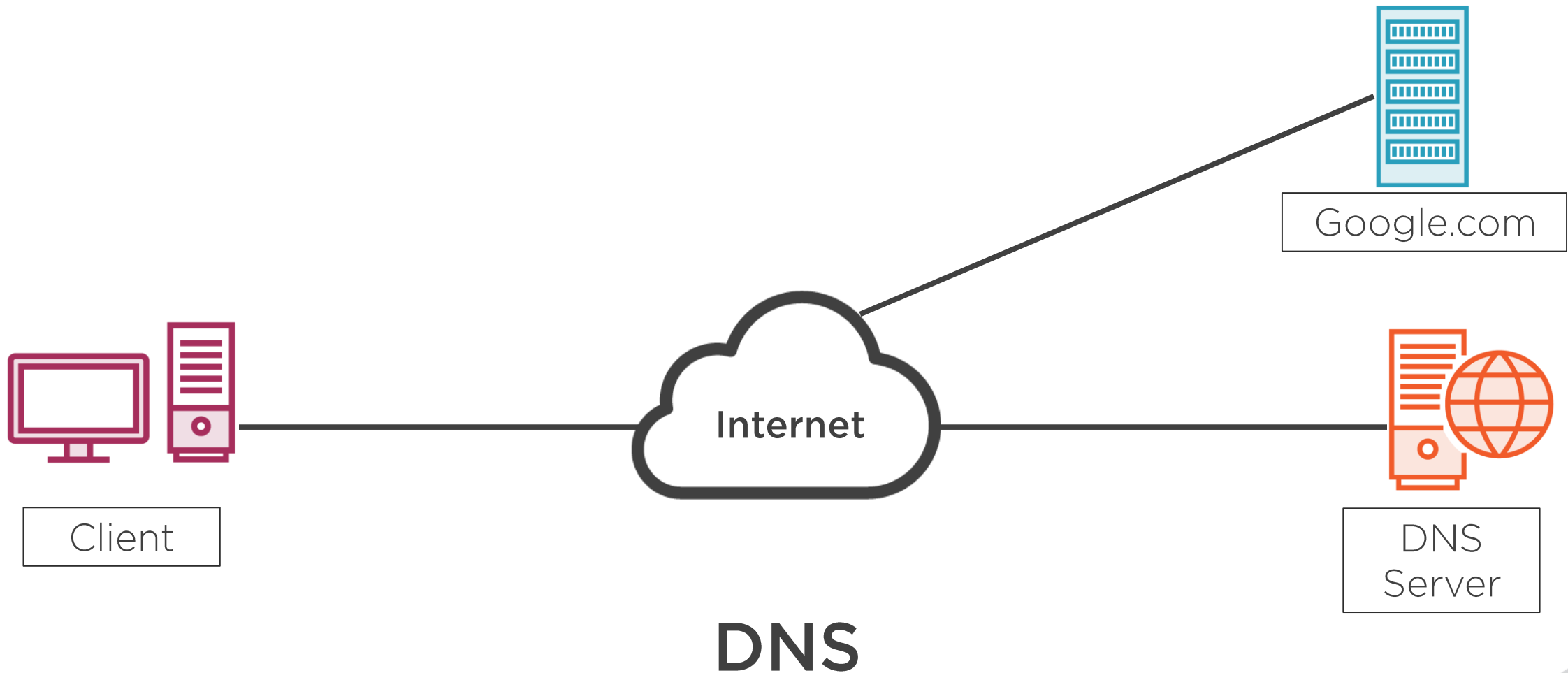
IP configuration via DHCP

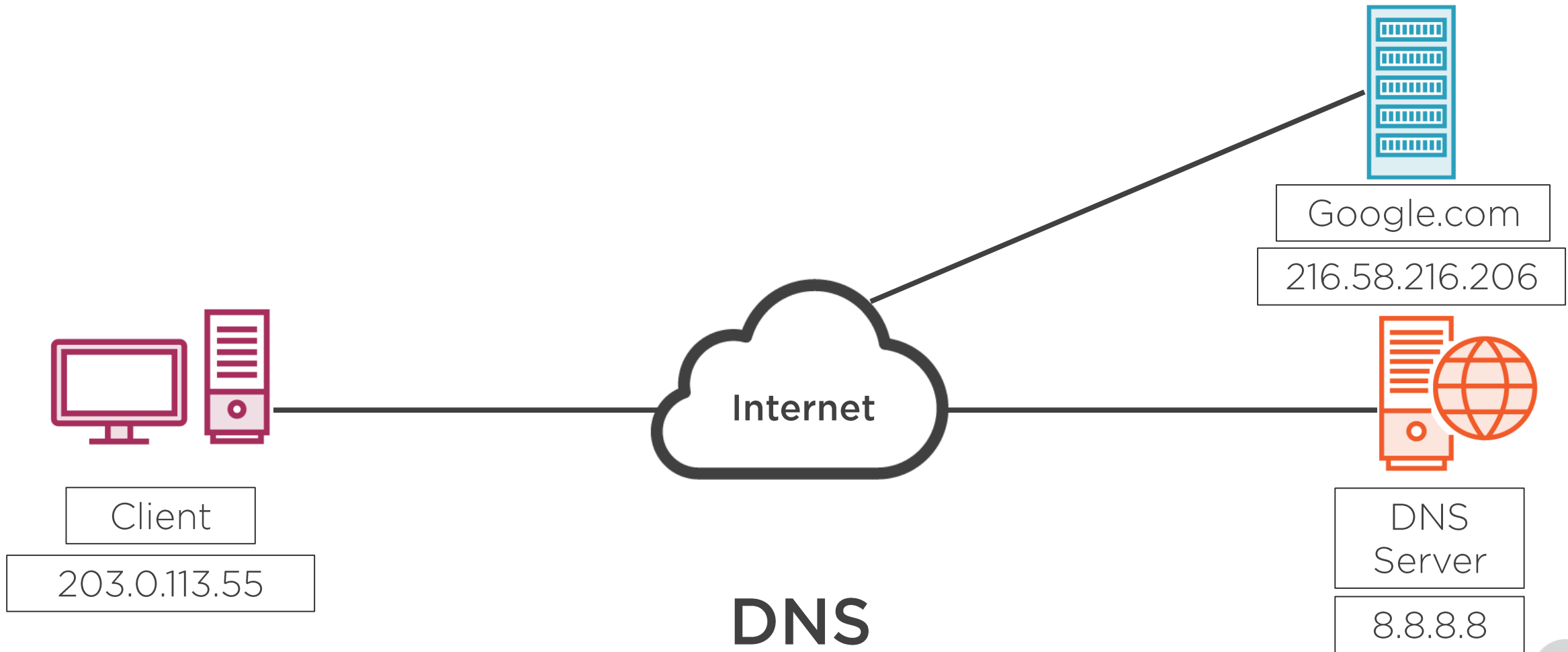


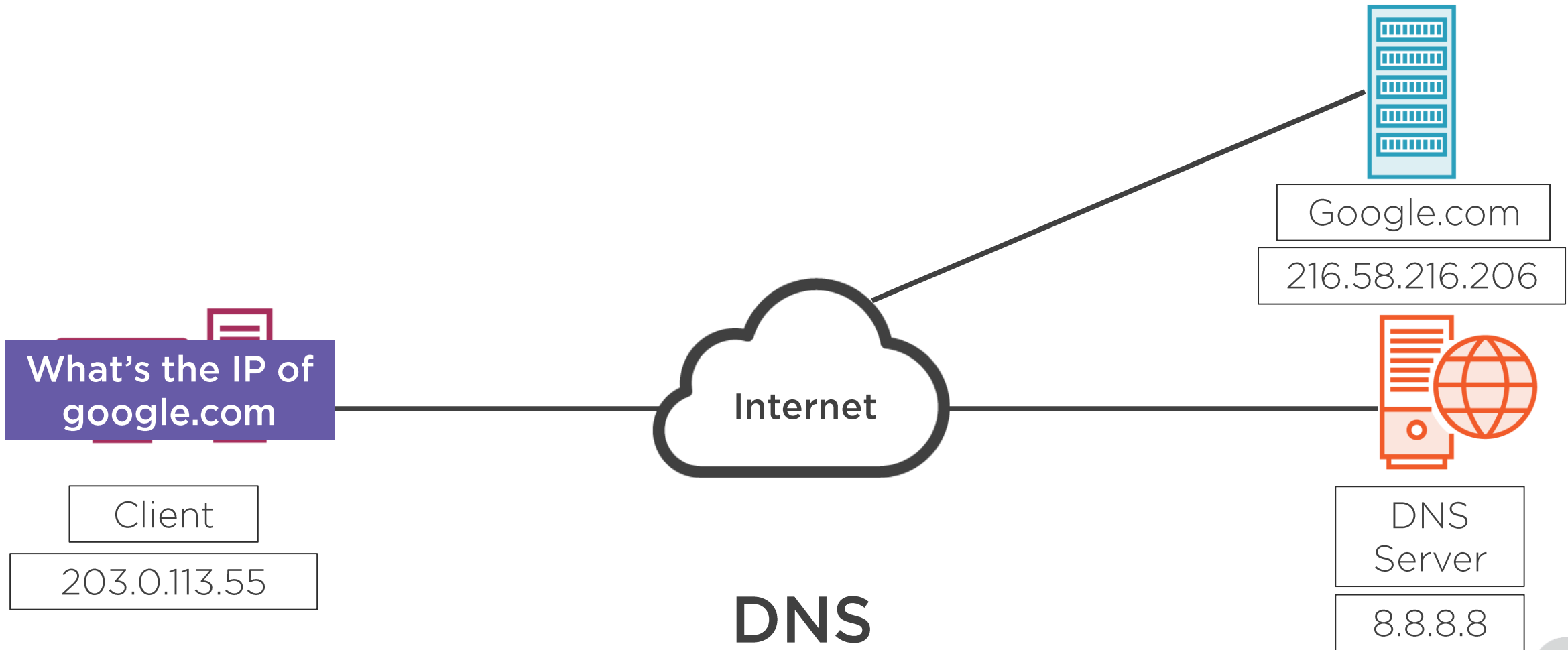


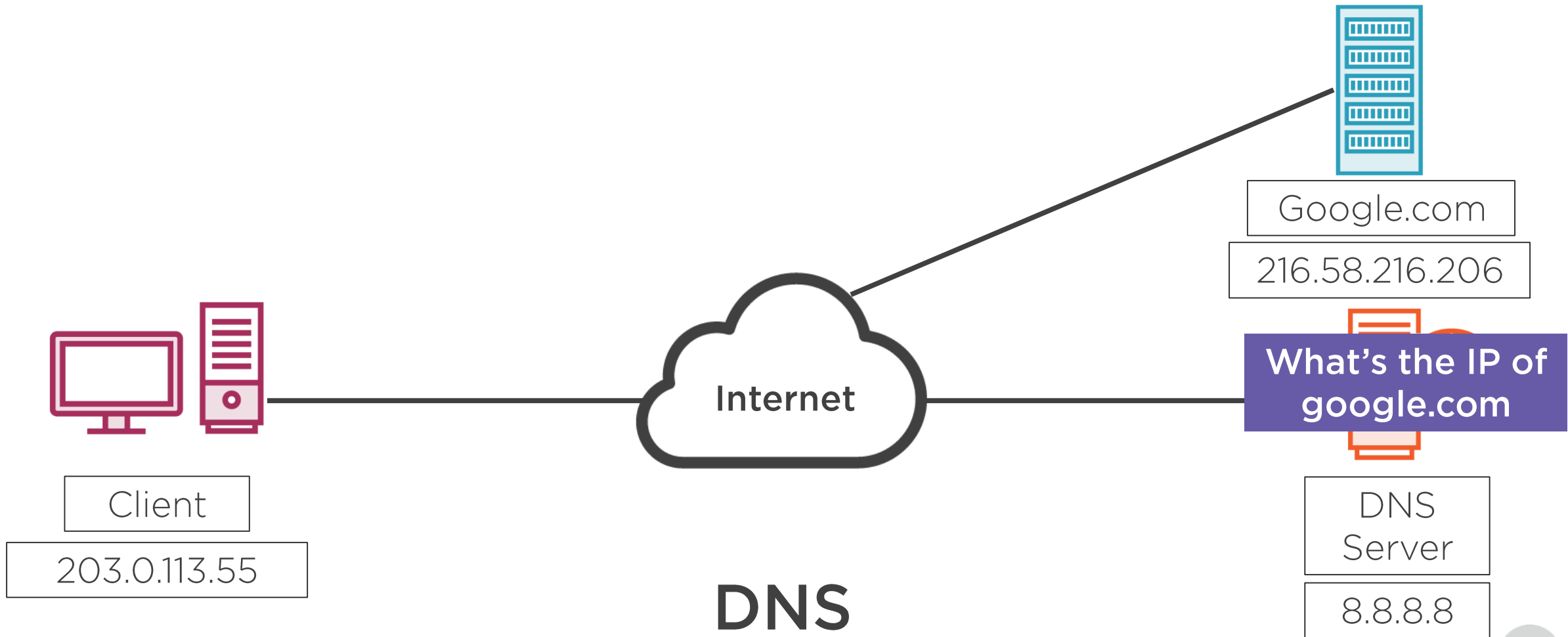
Domain Name System

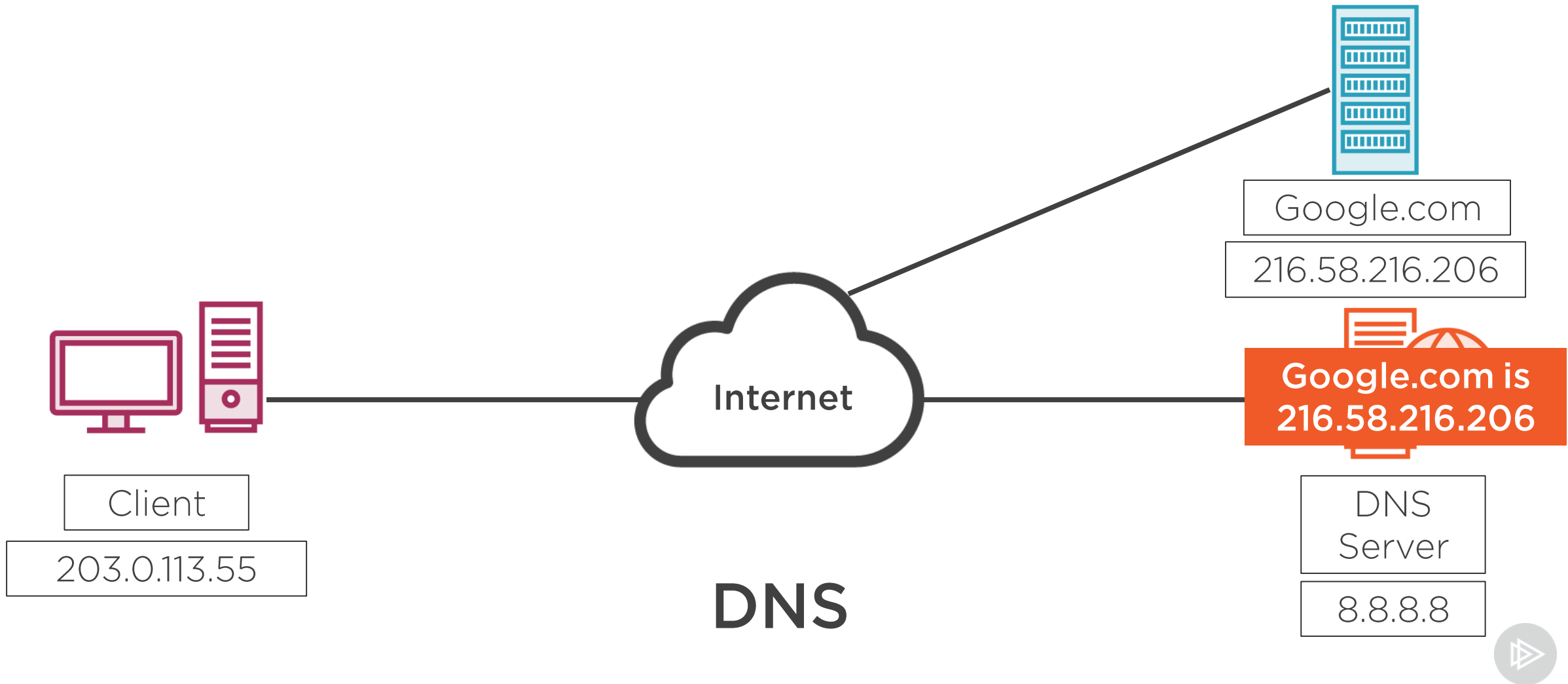


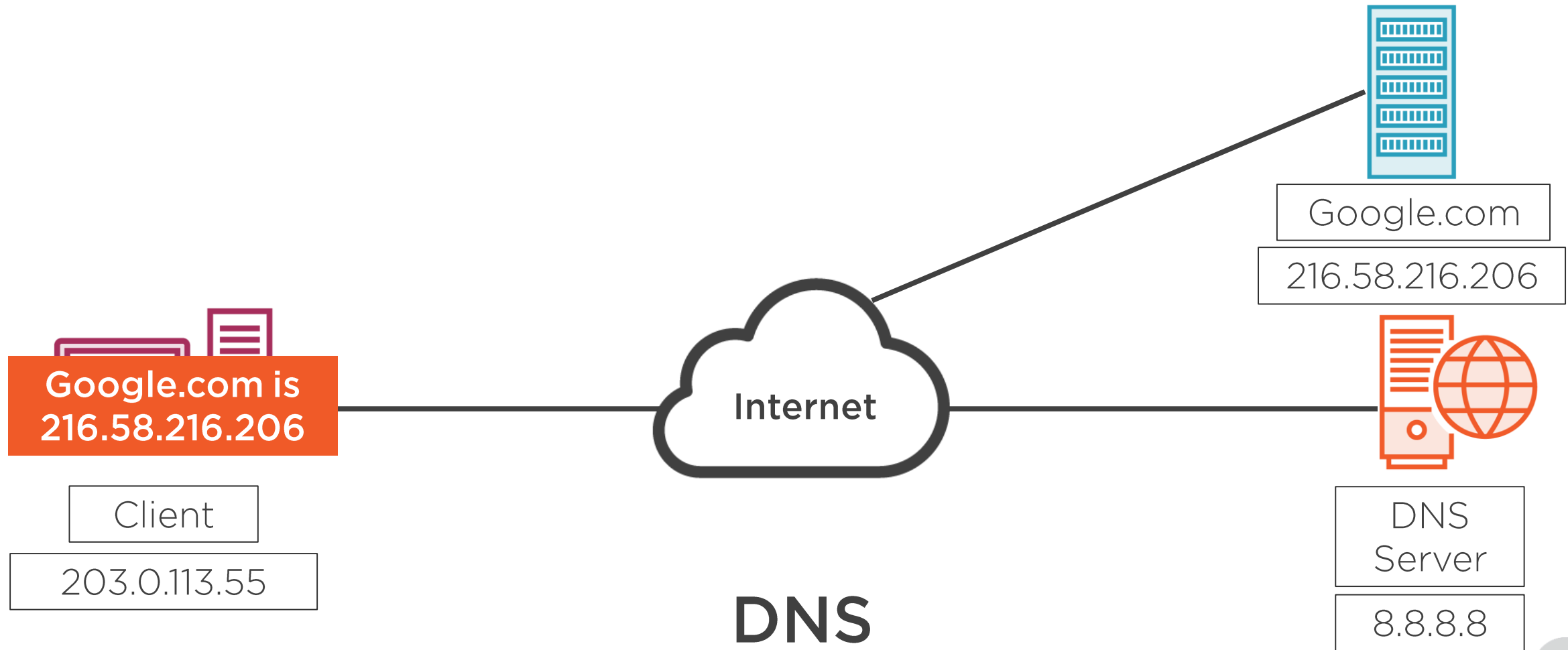


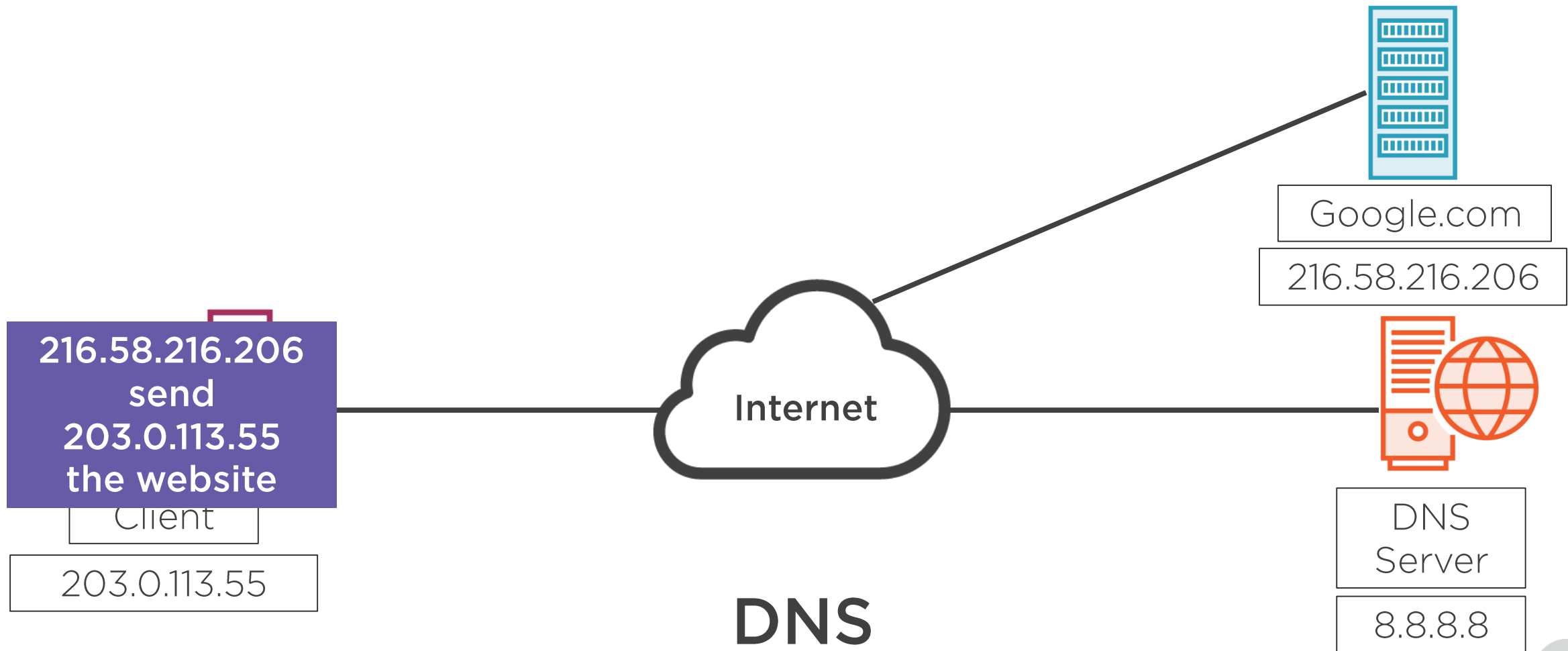


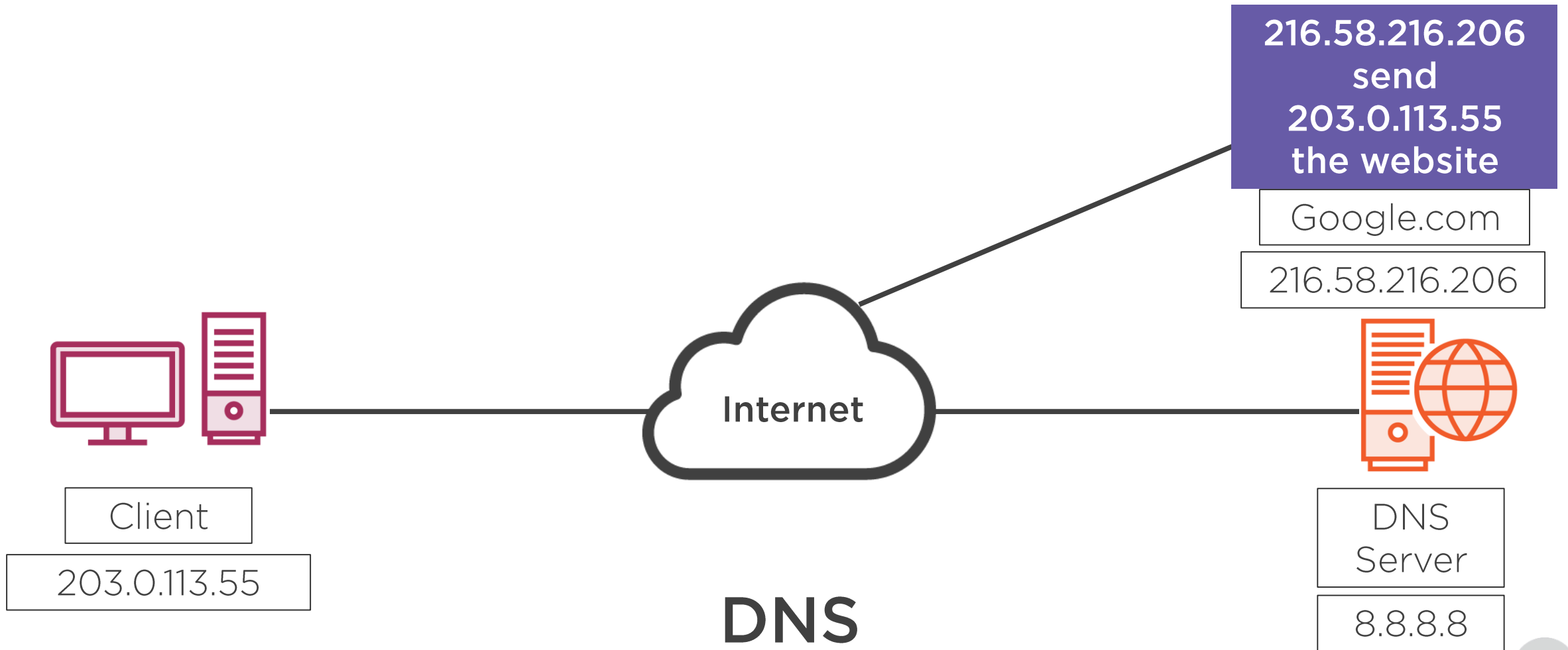


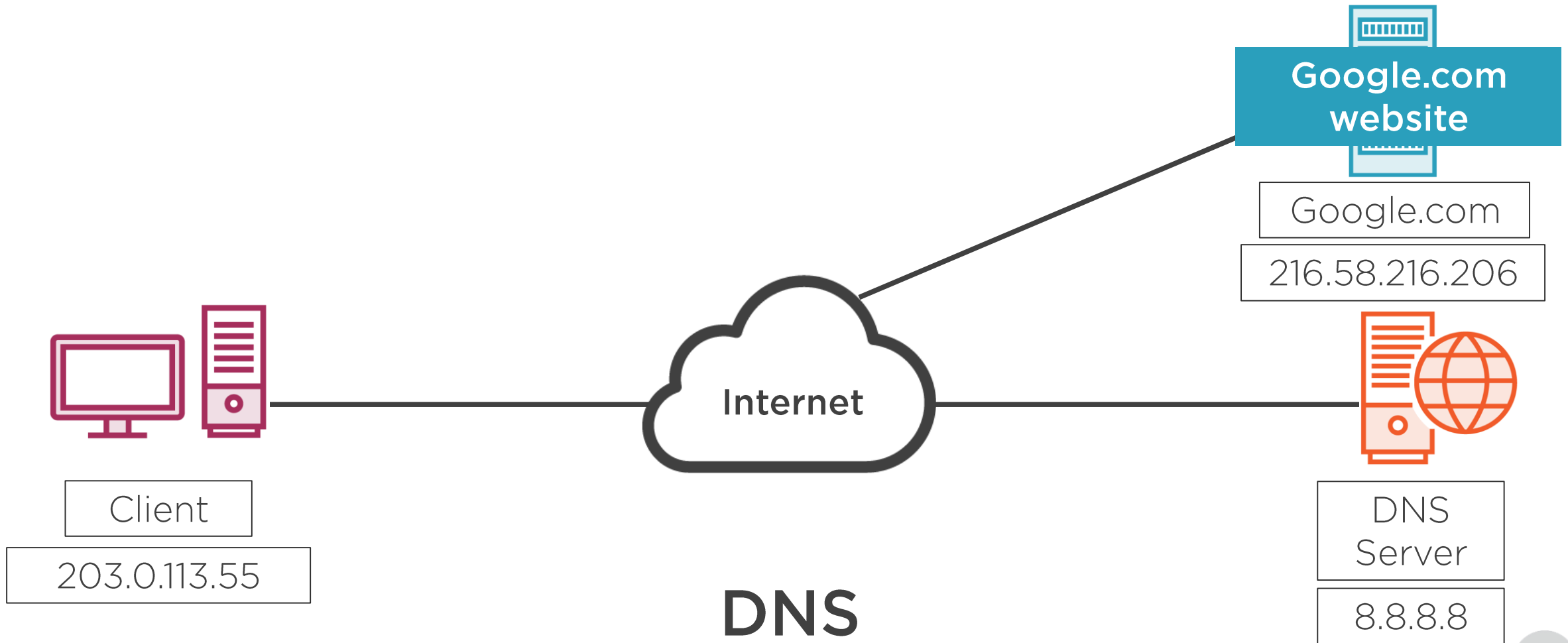


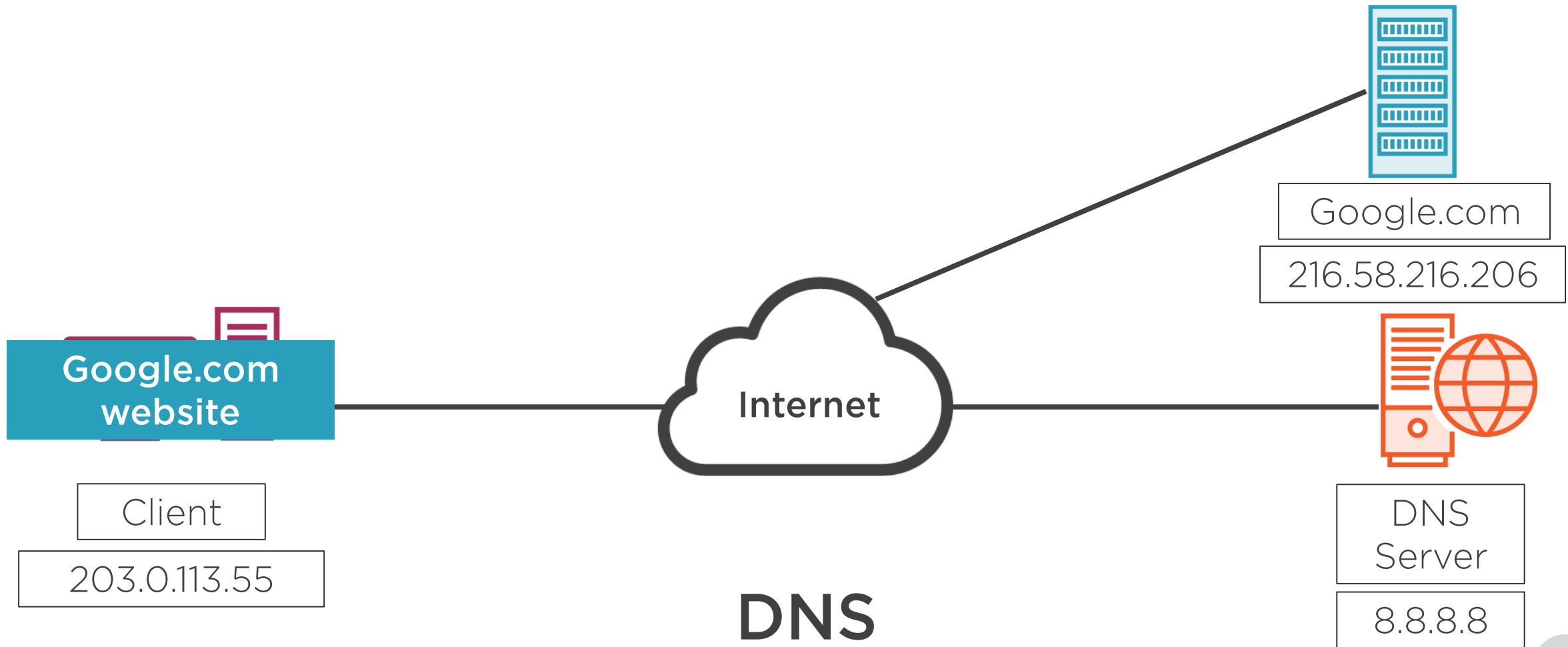












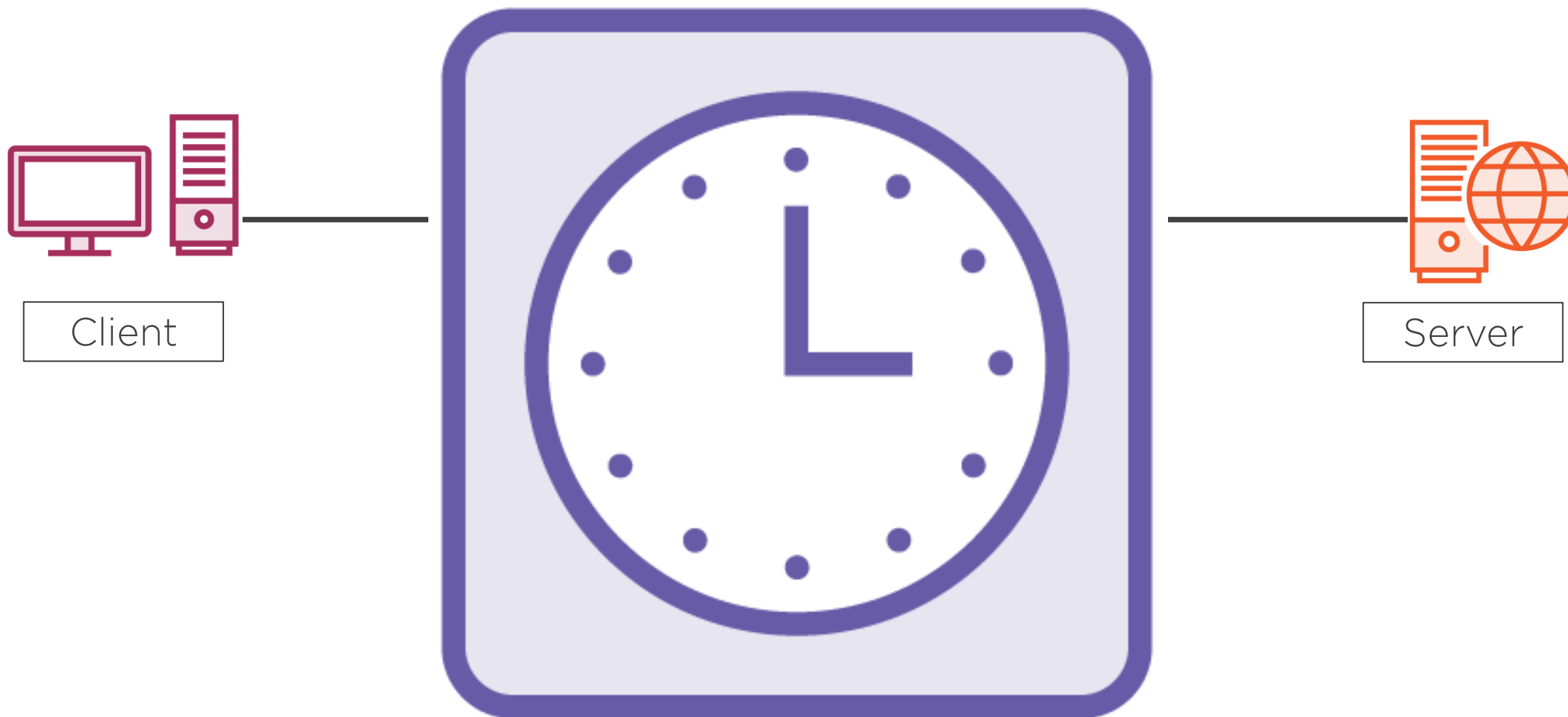
Demonstration:

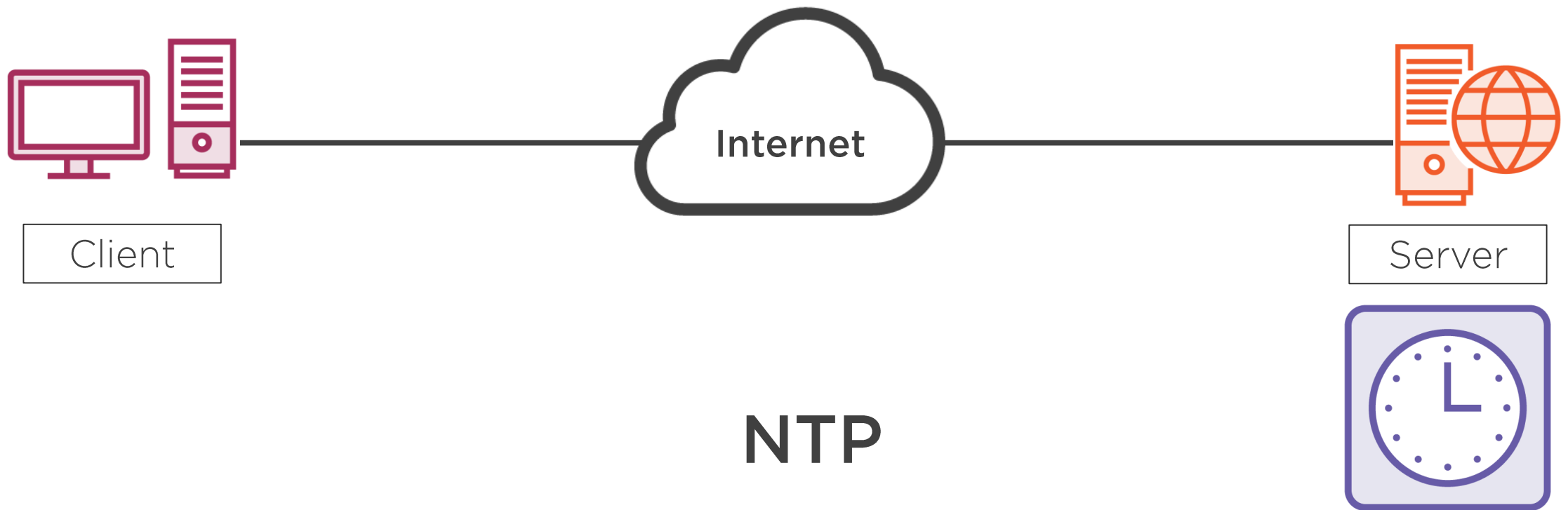
Examine DNS using nslookup

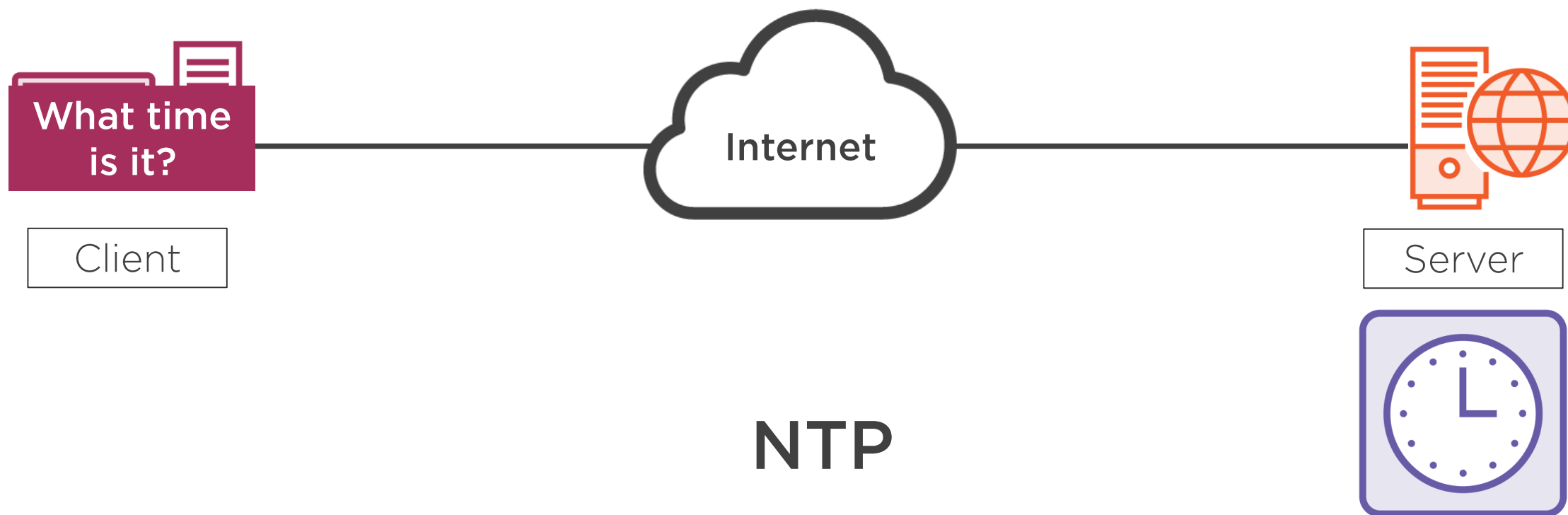


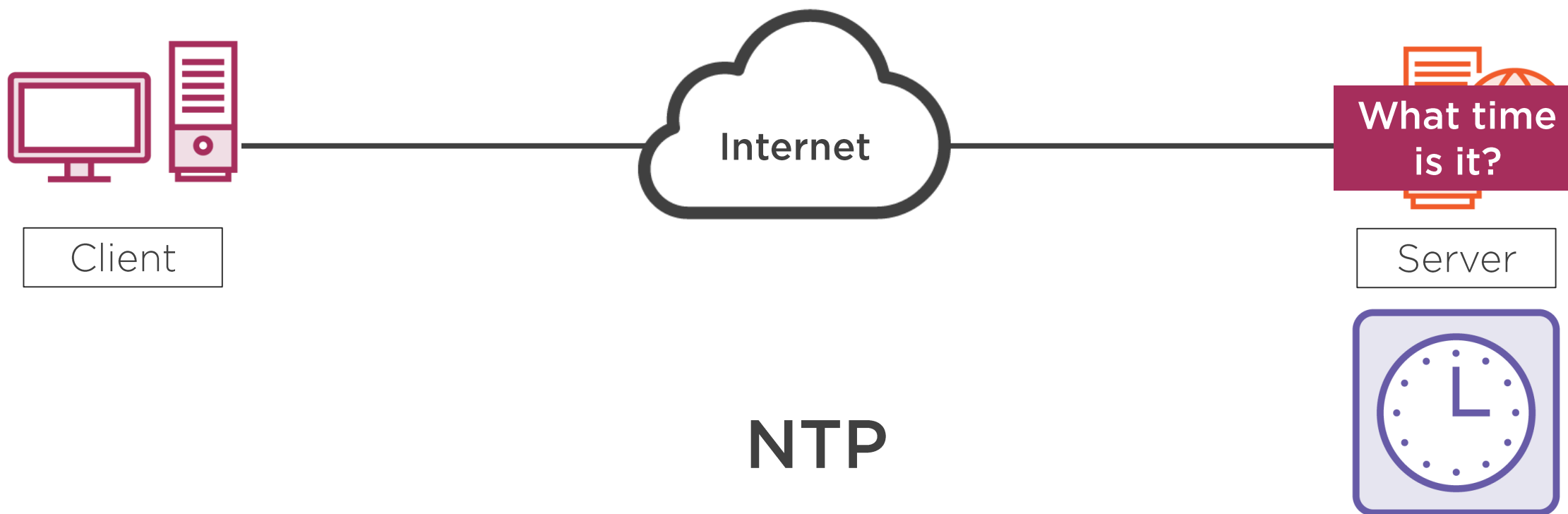


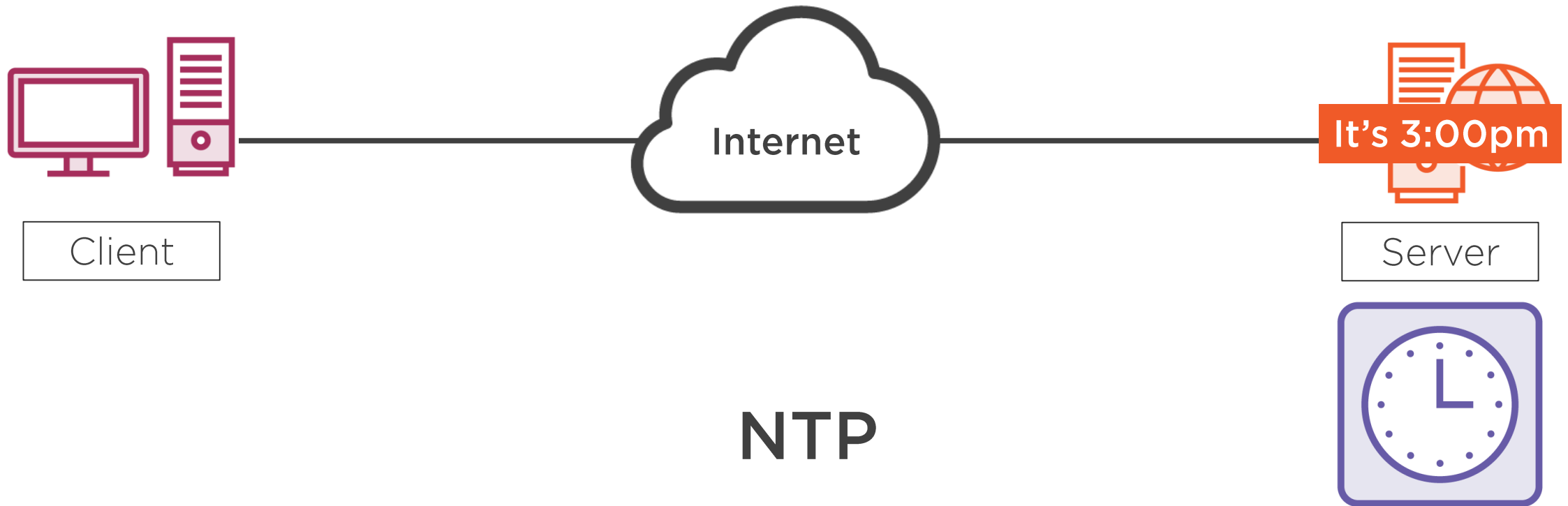
Network Time Protocol

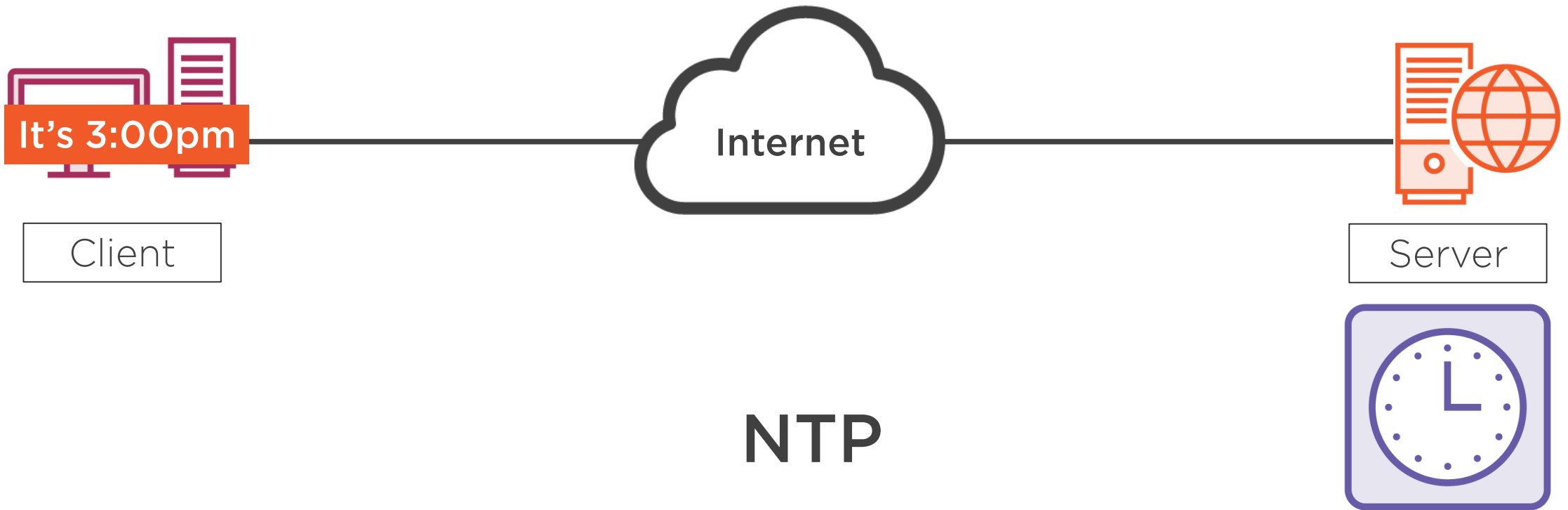








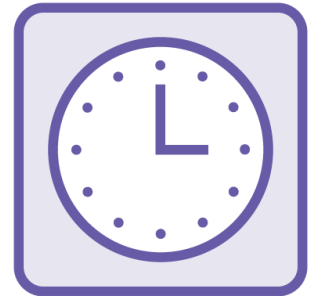


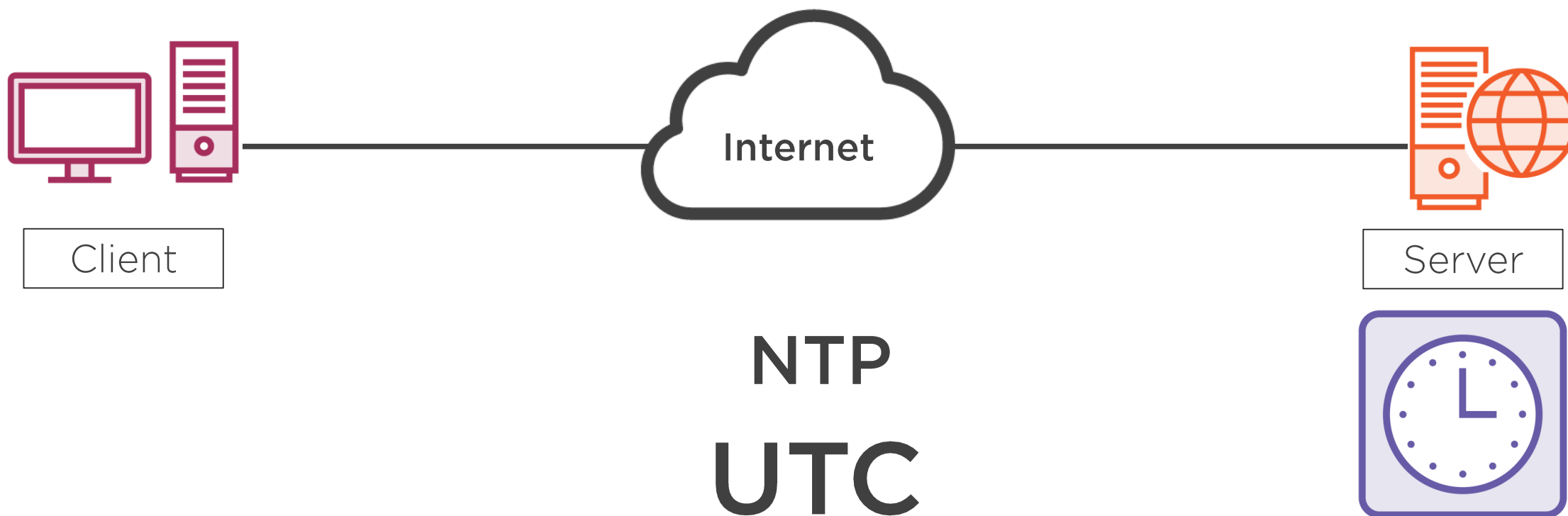




NTP

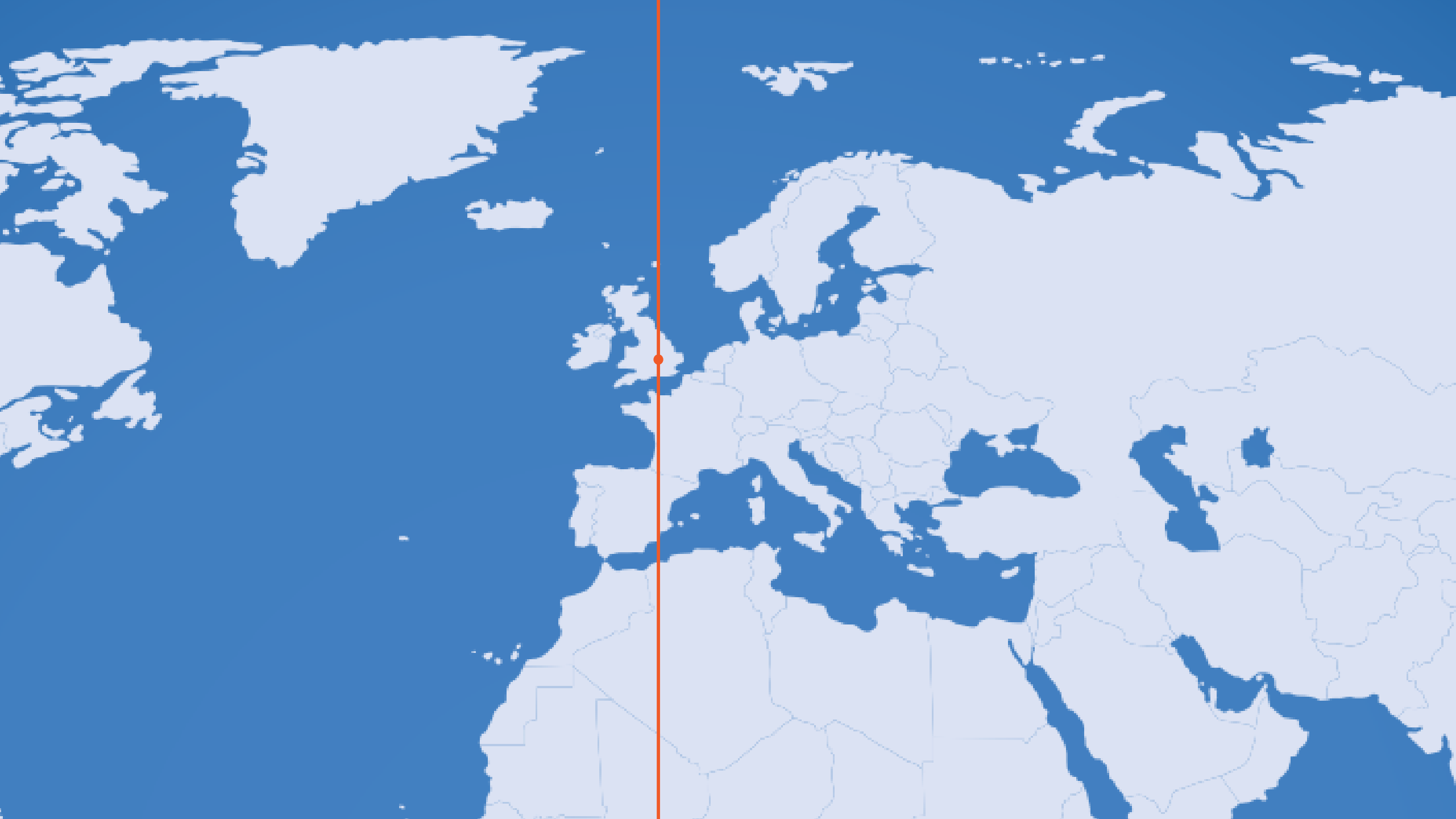
Coordinated Universal Time

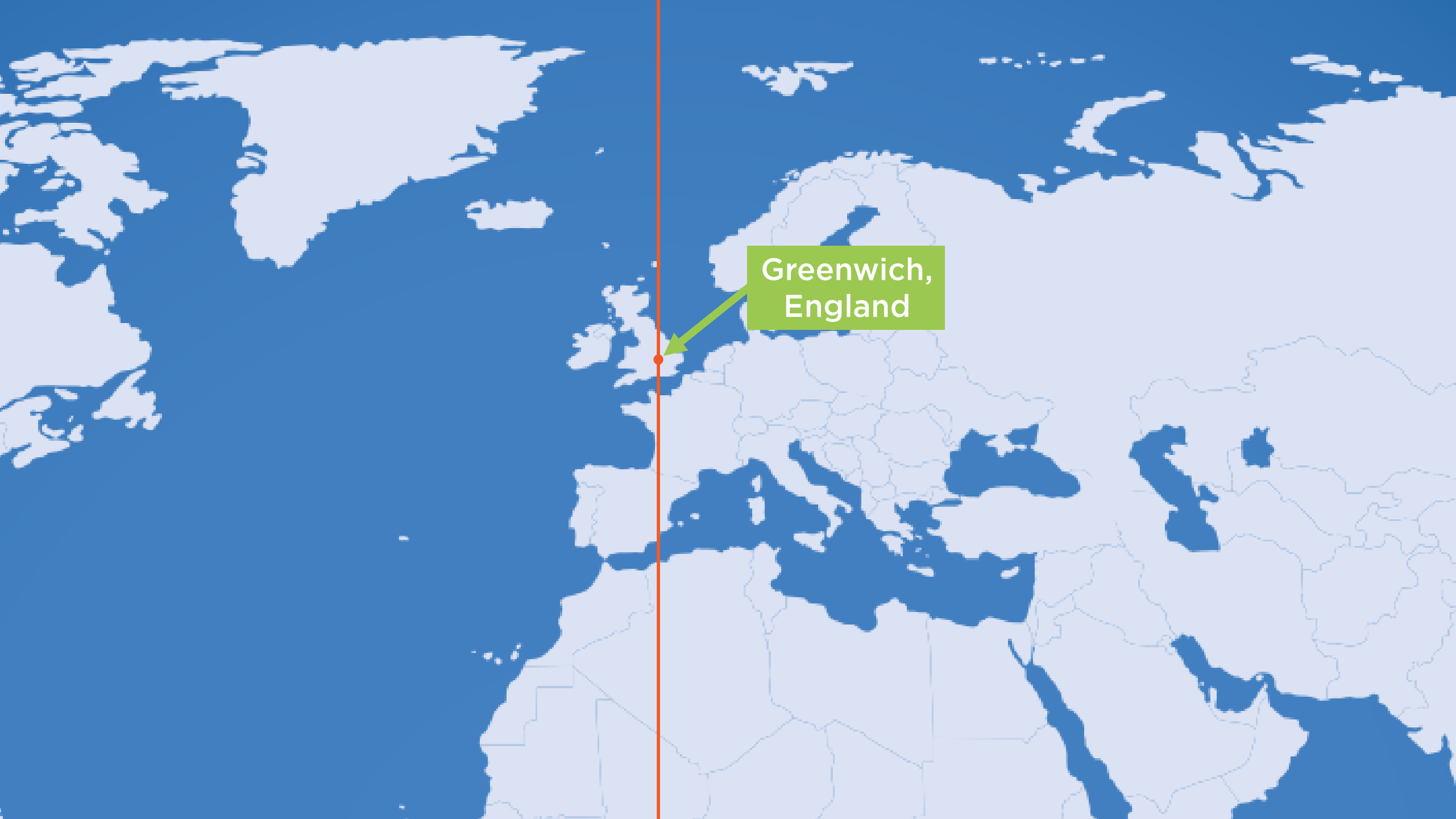












Greenwich,
England



Greenwich,
England

Prime Meridian



Greenwich,
England

Prime Meridian

Time at Midnight
00:00

A stylized world map with a dark blue ocean and light blue landmasses. A vertical red line runs through the center of the map, representing the Prime Meridian. The map is shown in a cylindrical projection.

Time at Midnight
00:00



A world map with a blue background and light blue landmasses. Two vertical red lines are drawn across the map, one through North America and one through Europe. Two orange text boxes are overlaid on the map. The first box, on the left, contains the text 'Chicago -06:00 (no DST)'. The second box, in the center, contains the text 'Time at Midnight 00:00'.

Chicago
-06:00
(no DST)

Time at Midnight
00:00



A world map with a blue background and light blue landmasses. Two vertical orange lines are drawn across the map, one at approximately 105°W and another at approximately 15°W. An orange rectangular box is positioned on the left side of the map, and another orange rectangular box is positioned in the lower center of the map.

Utah
-07:00
(no DST)

Time at Midnight
00:00

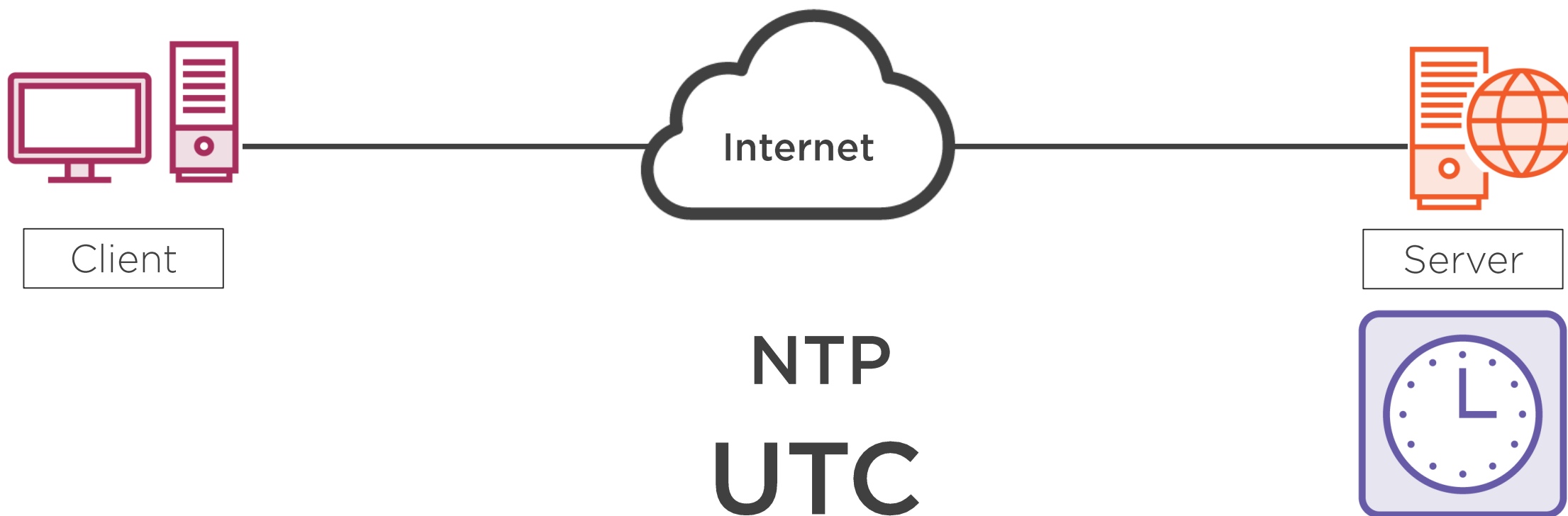


A world map with a blue background and white landmasses. Two vertical red lines are drawn across the map. The first line is positioned over the Atlantic Ocean, and the second line is positioned over the Indian Ocean. An orange rectangular box is located in the lower-left quadrant, and another orange rectangular box is located in the upper-right quadrant.

New Delhi
+05:30
(no DST)

Time at Midnight
00:00





Network Management





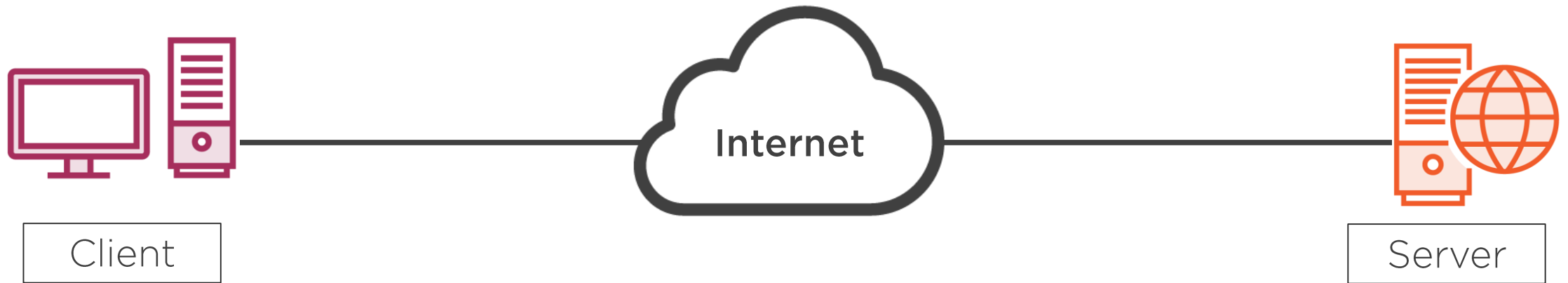
Telnet

Secure Shell



Telnet

SSH



Telnet

SSH
encrypted



Telnet
23

SSH
22



Network
Administrator
Workstation



Client

Network

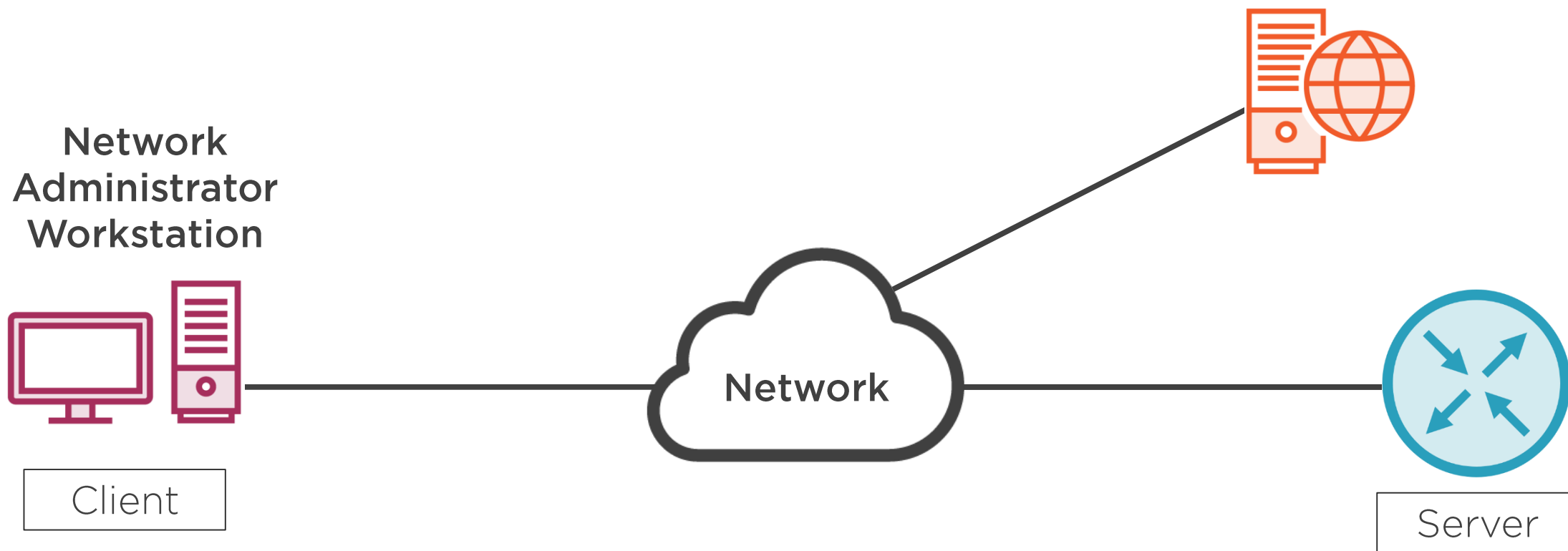


Server

Telnet

SSH

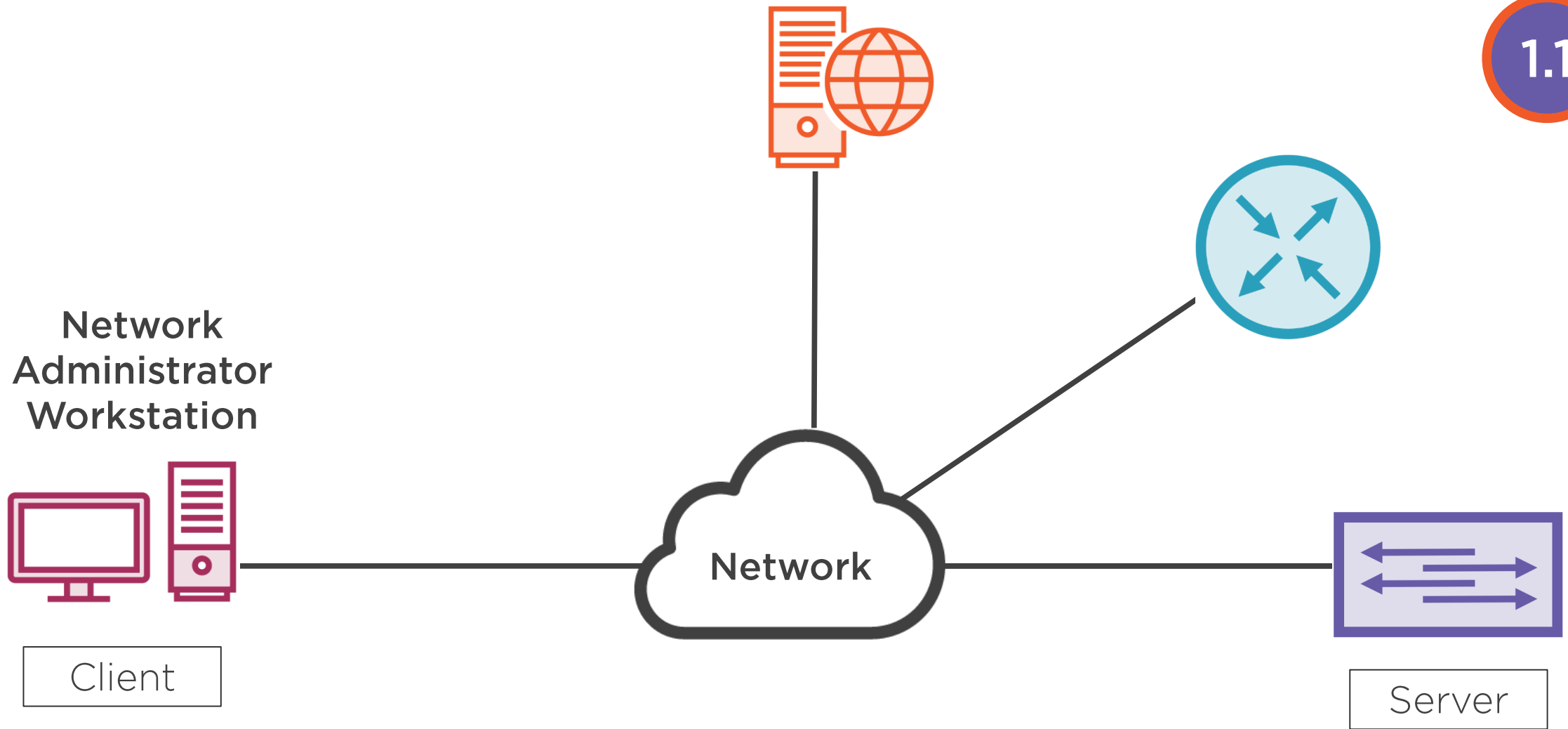




Telnet

SSH

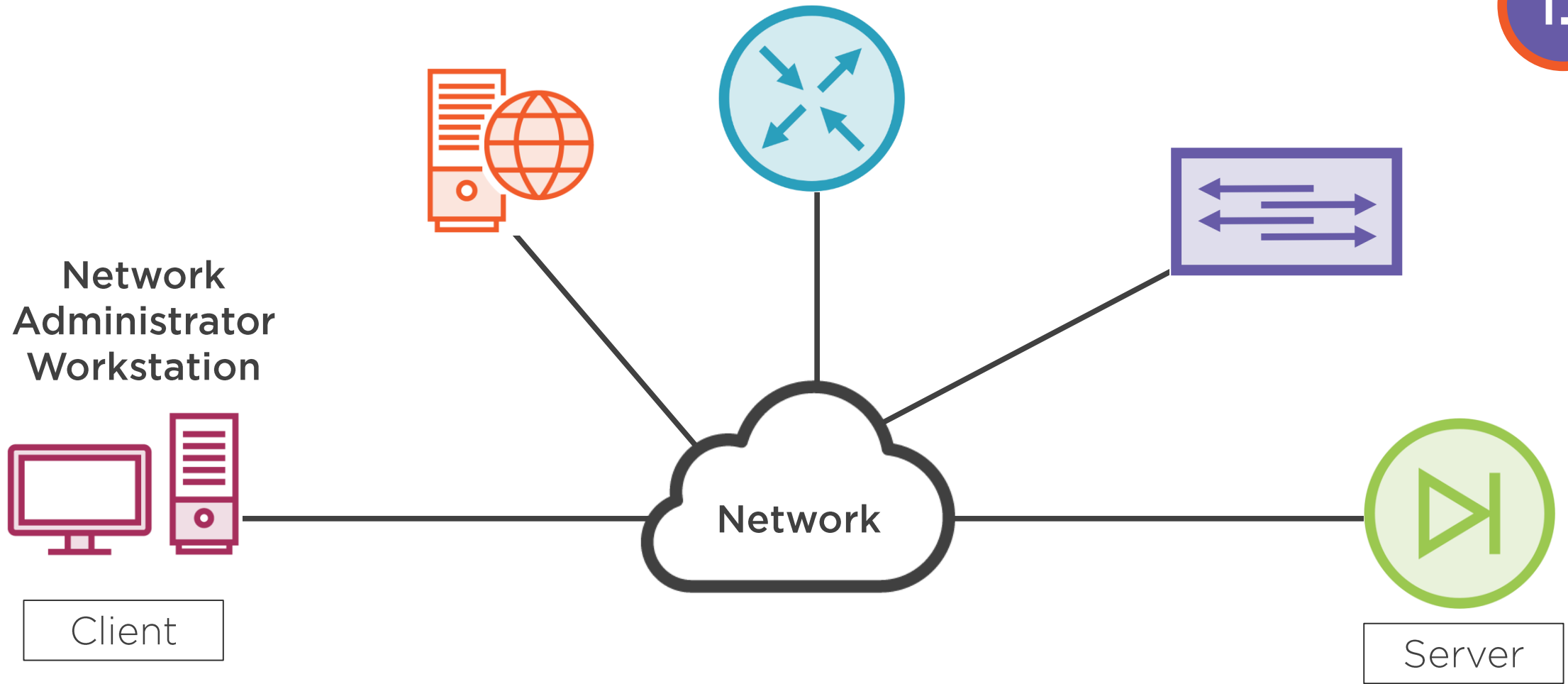




Telnet

SSH





Telnet

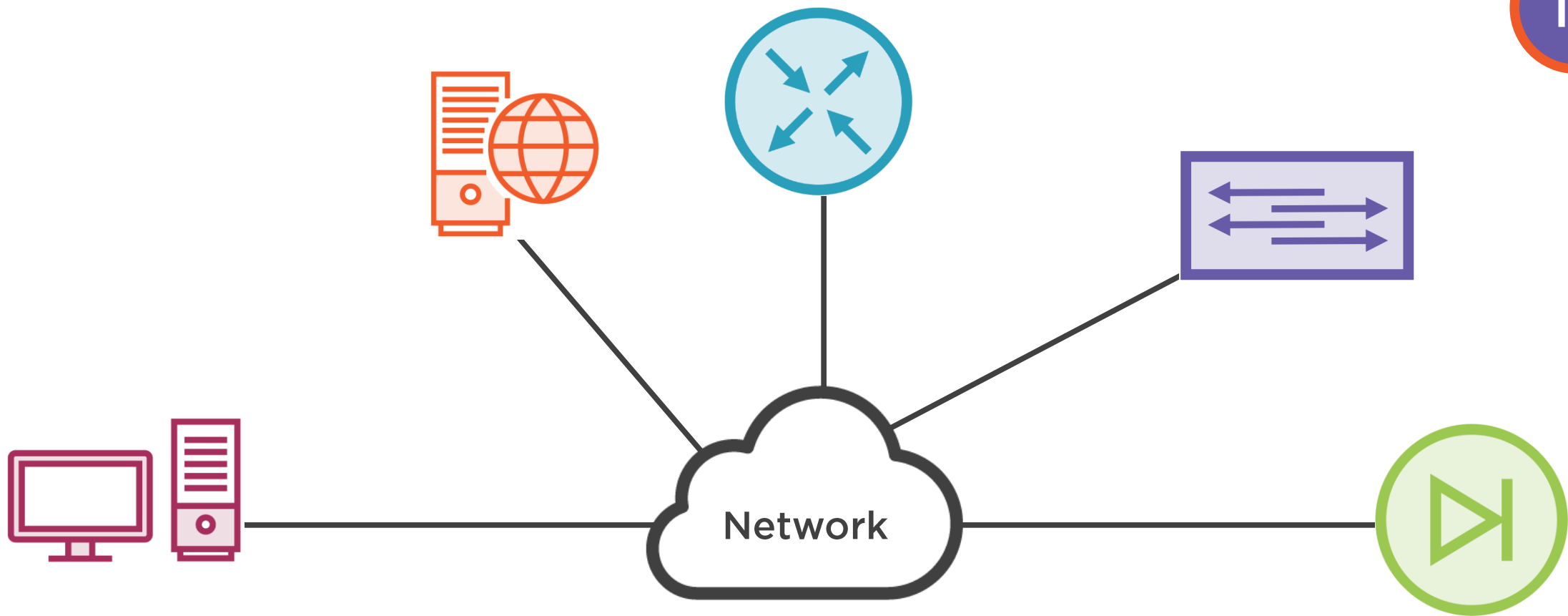
SSH



Demonstration:

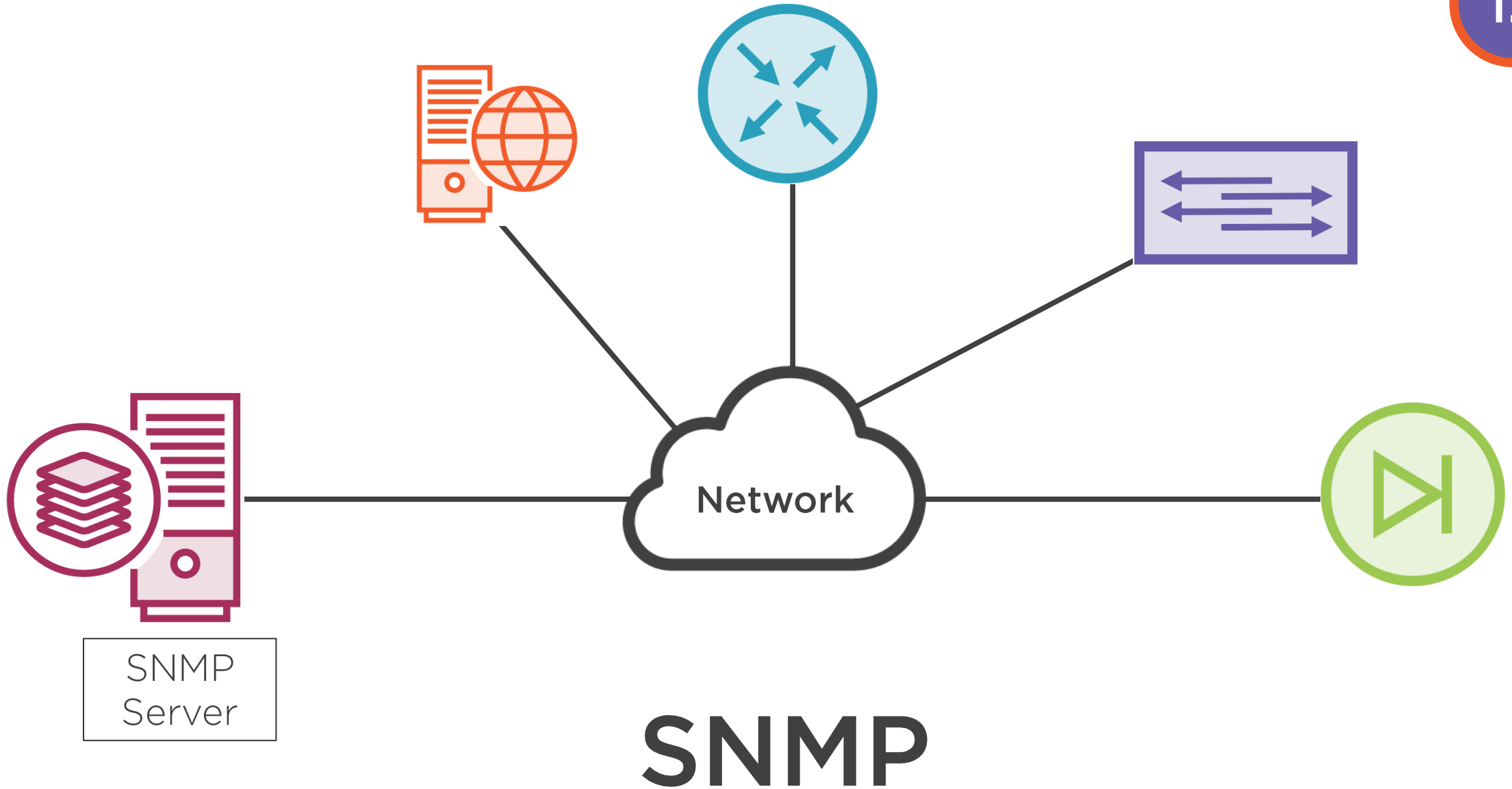
Examine SSH use

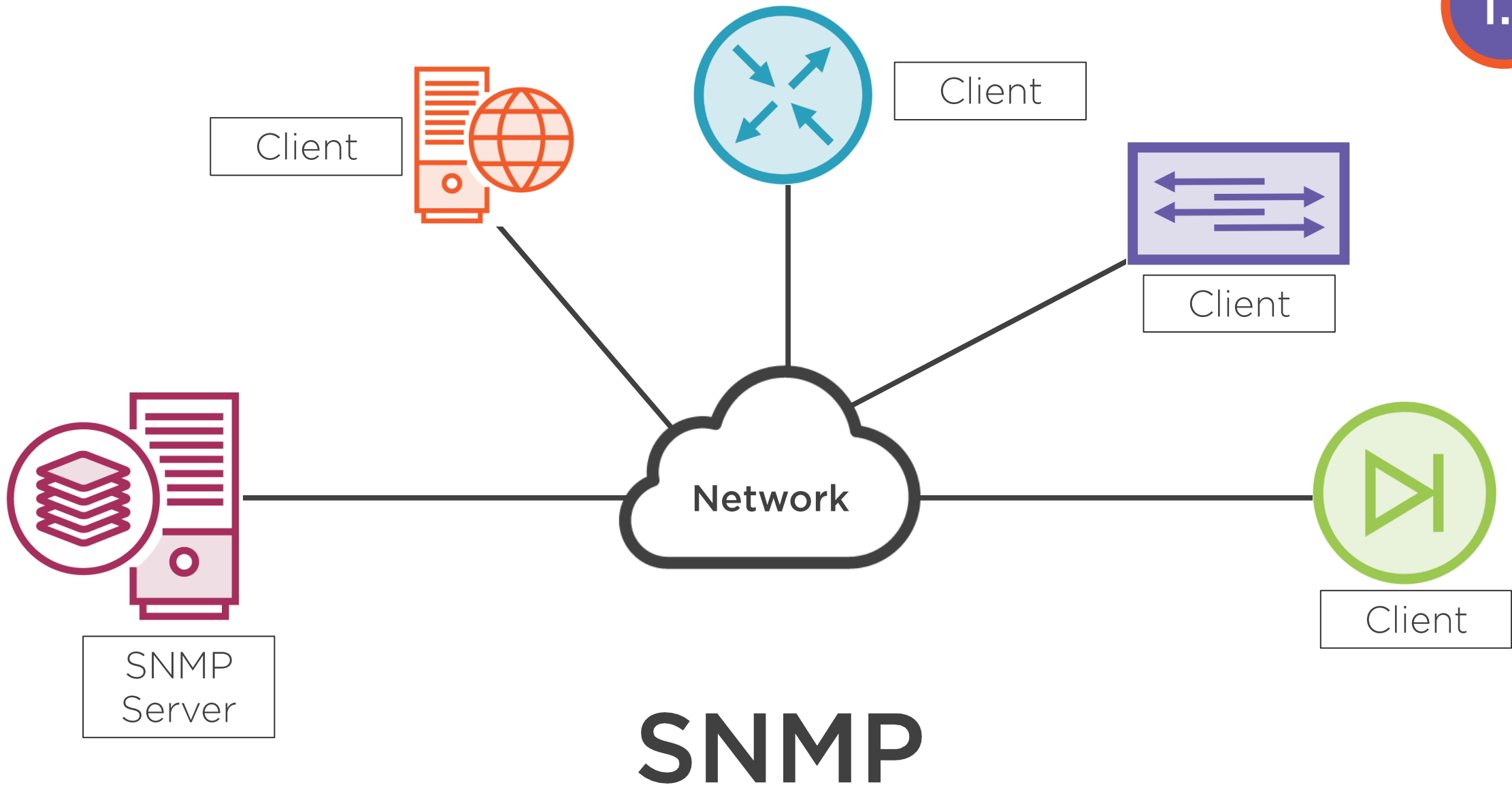


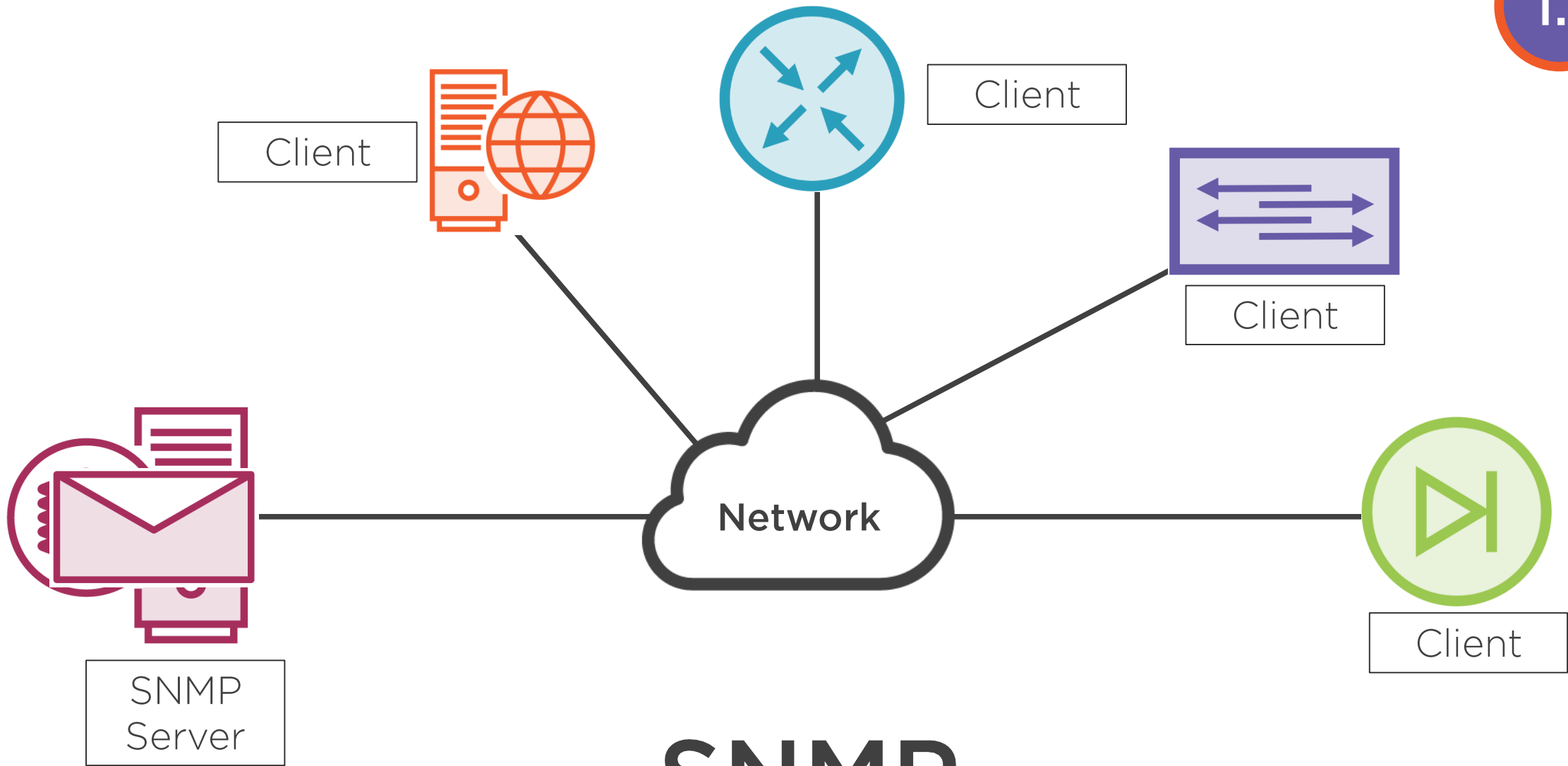


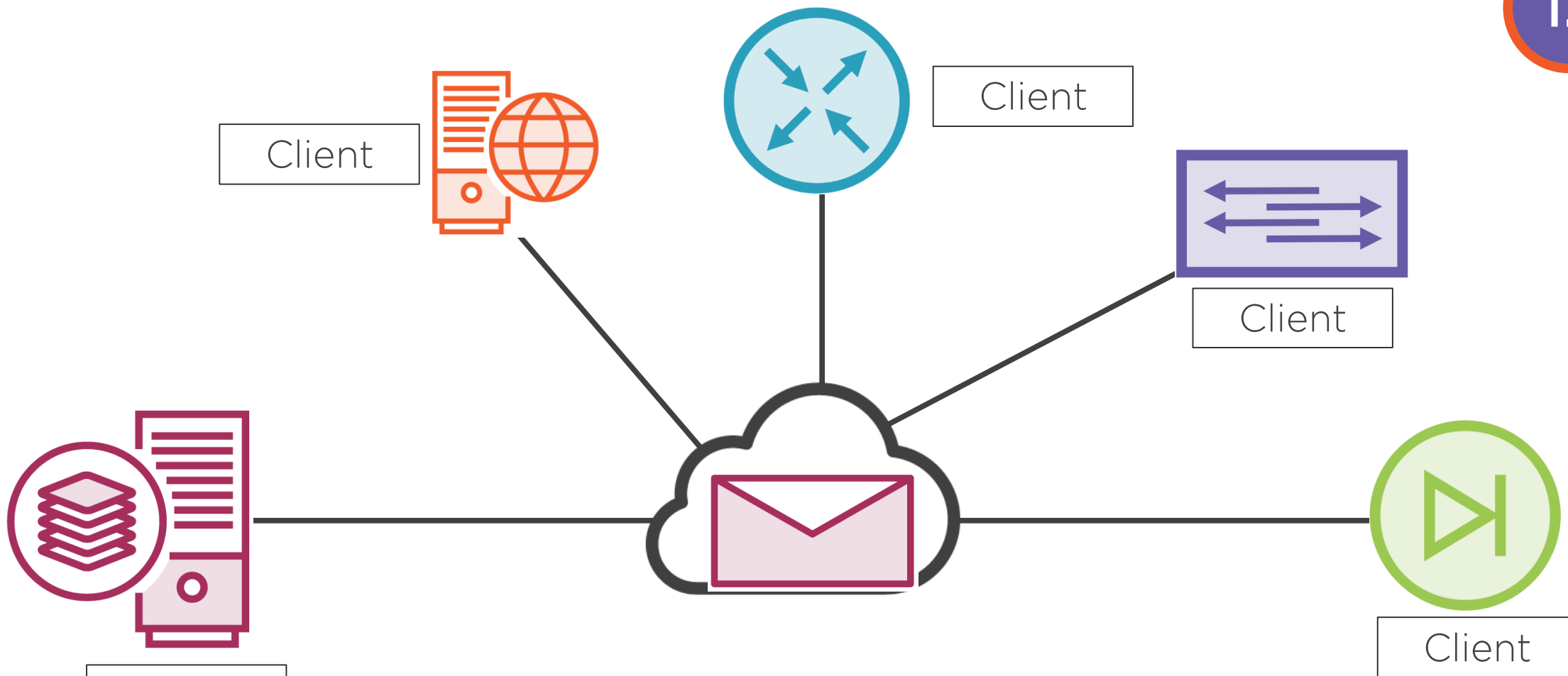
SNMP







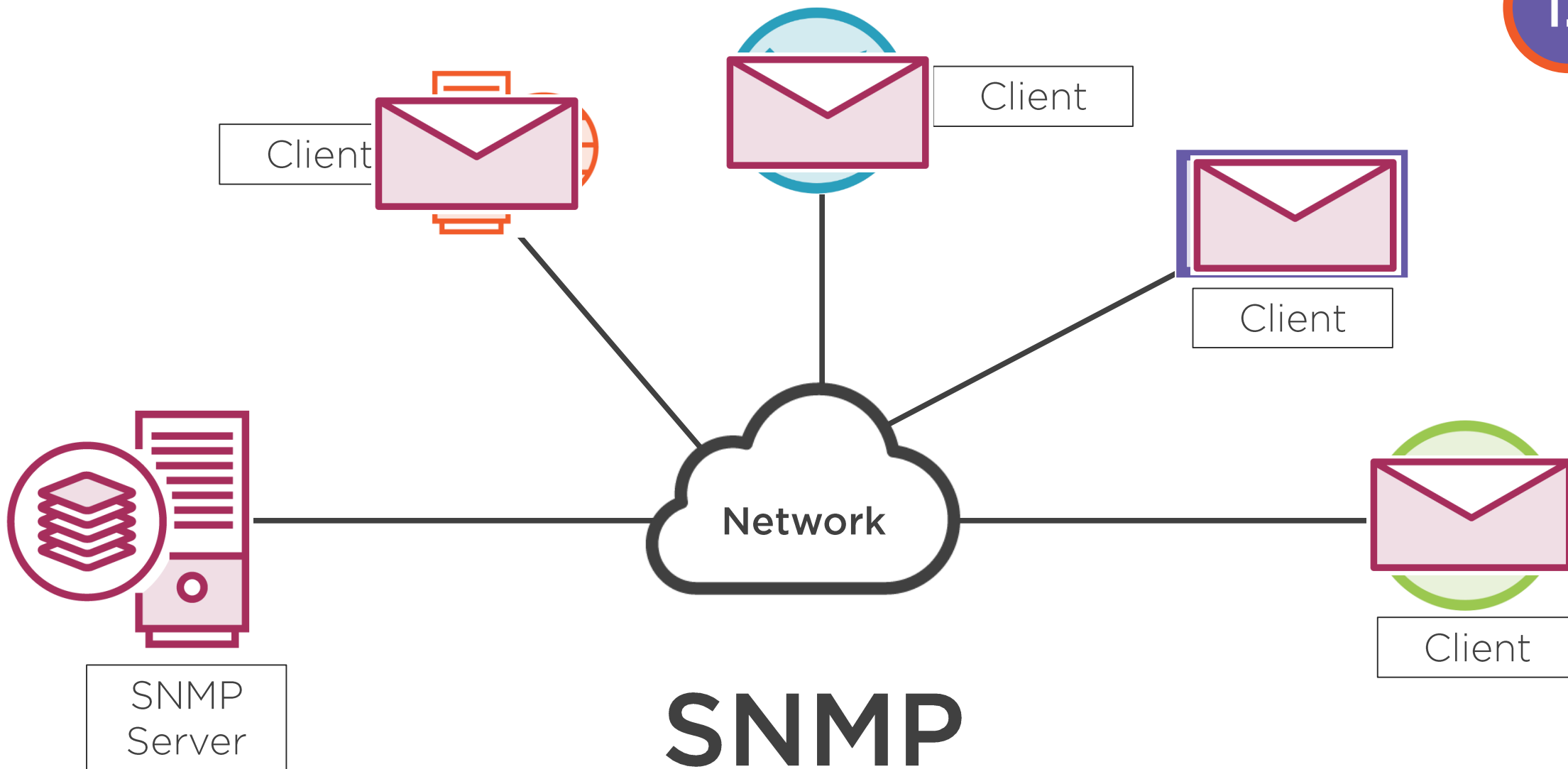




SNMP

“Walk the Tree”

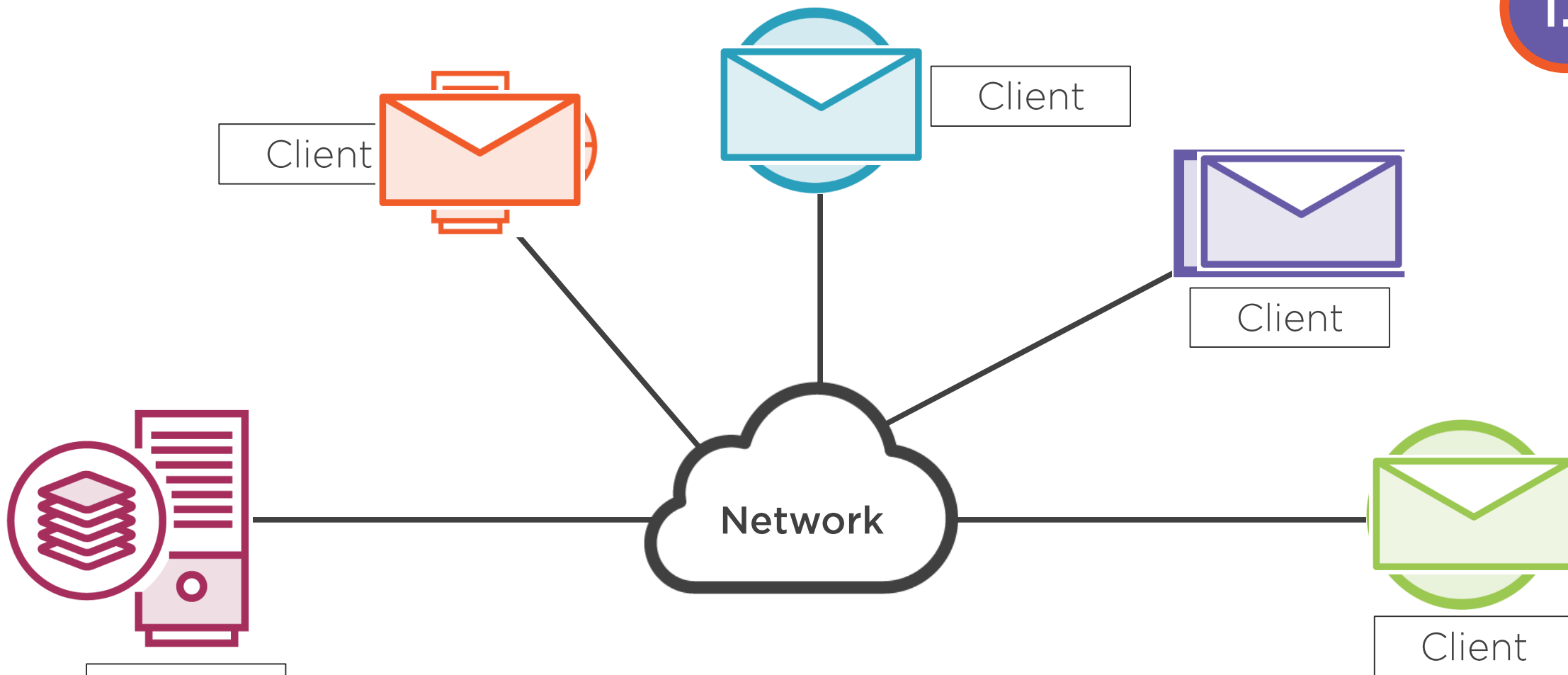




SNMP

“Walk the Tree”

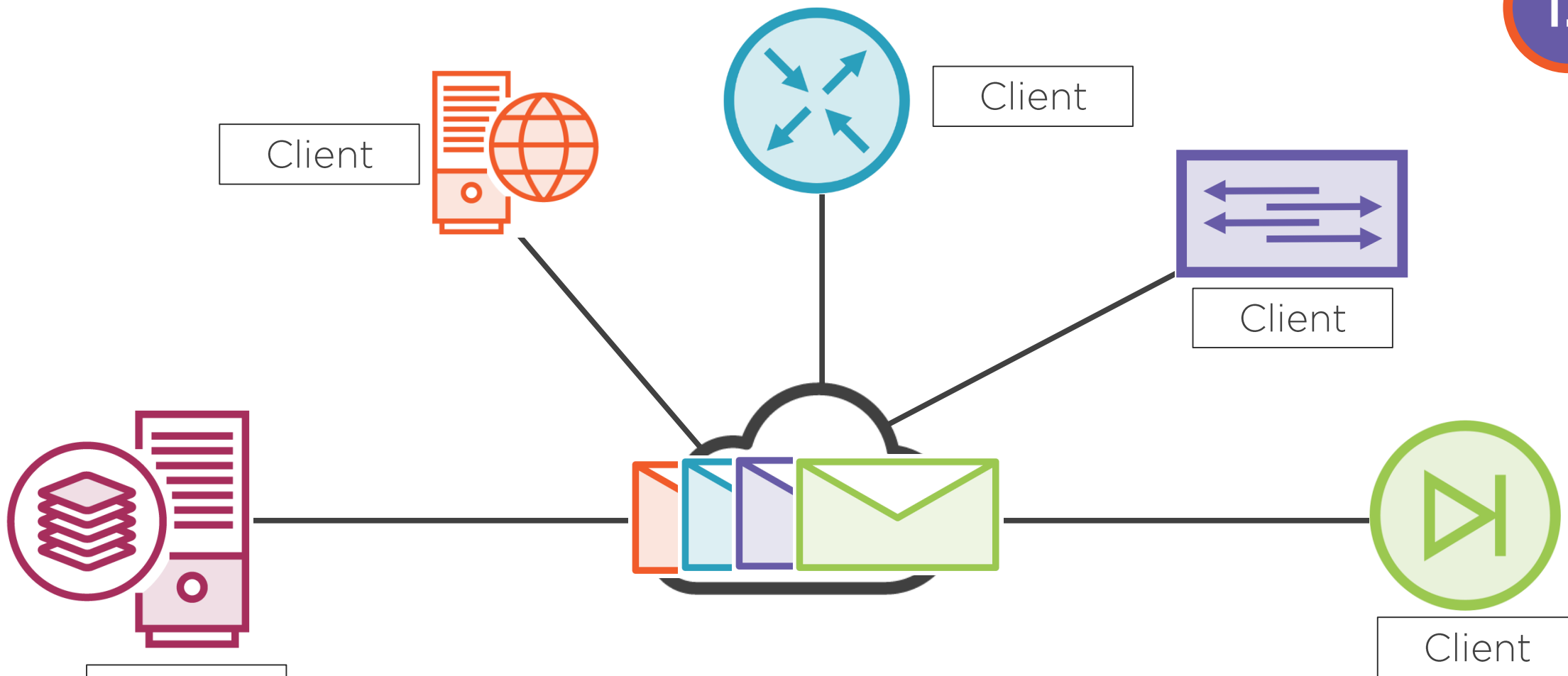




SNMP

“Walk the Tree”

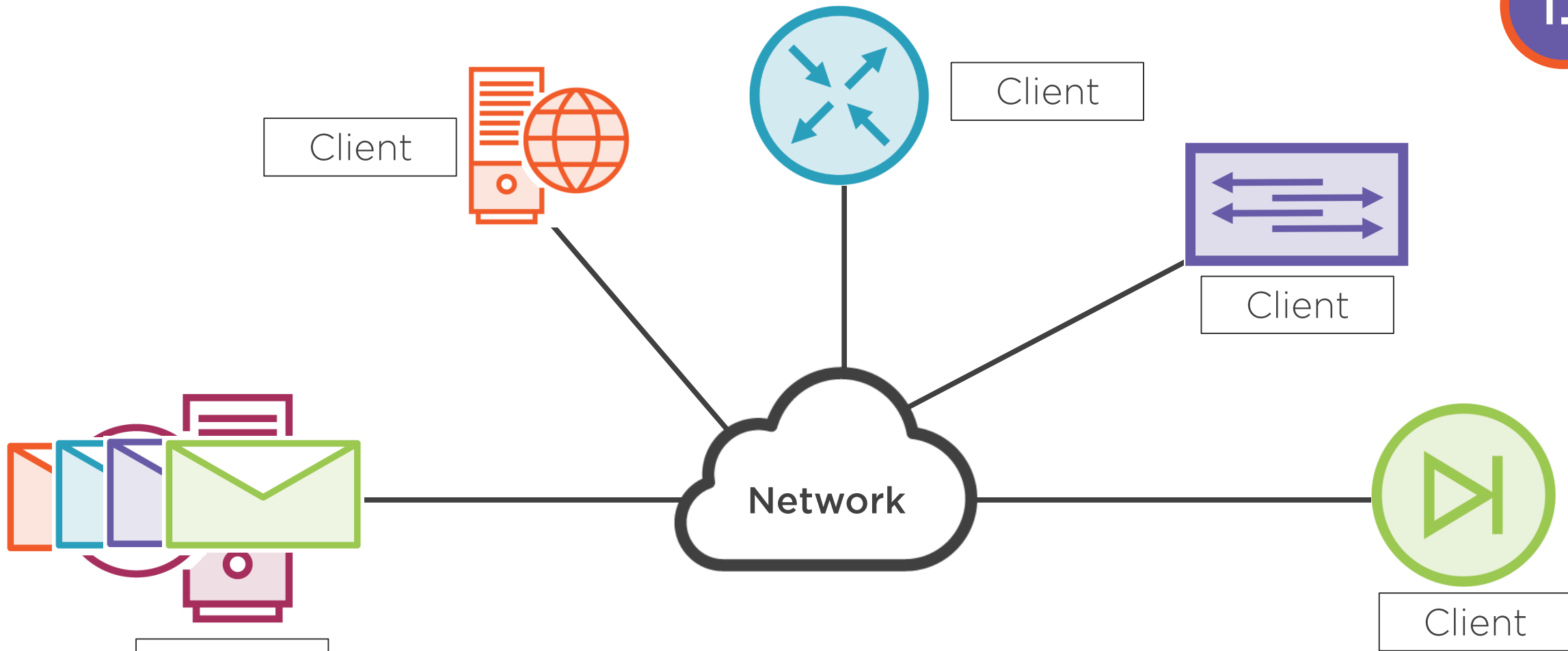




SNMP

"Walk the Tree"

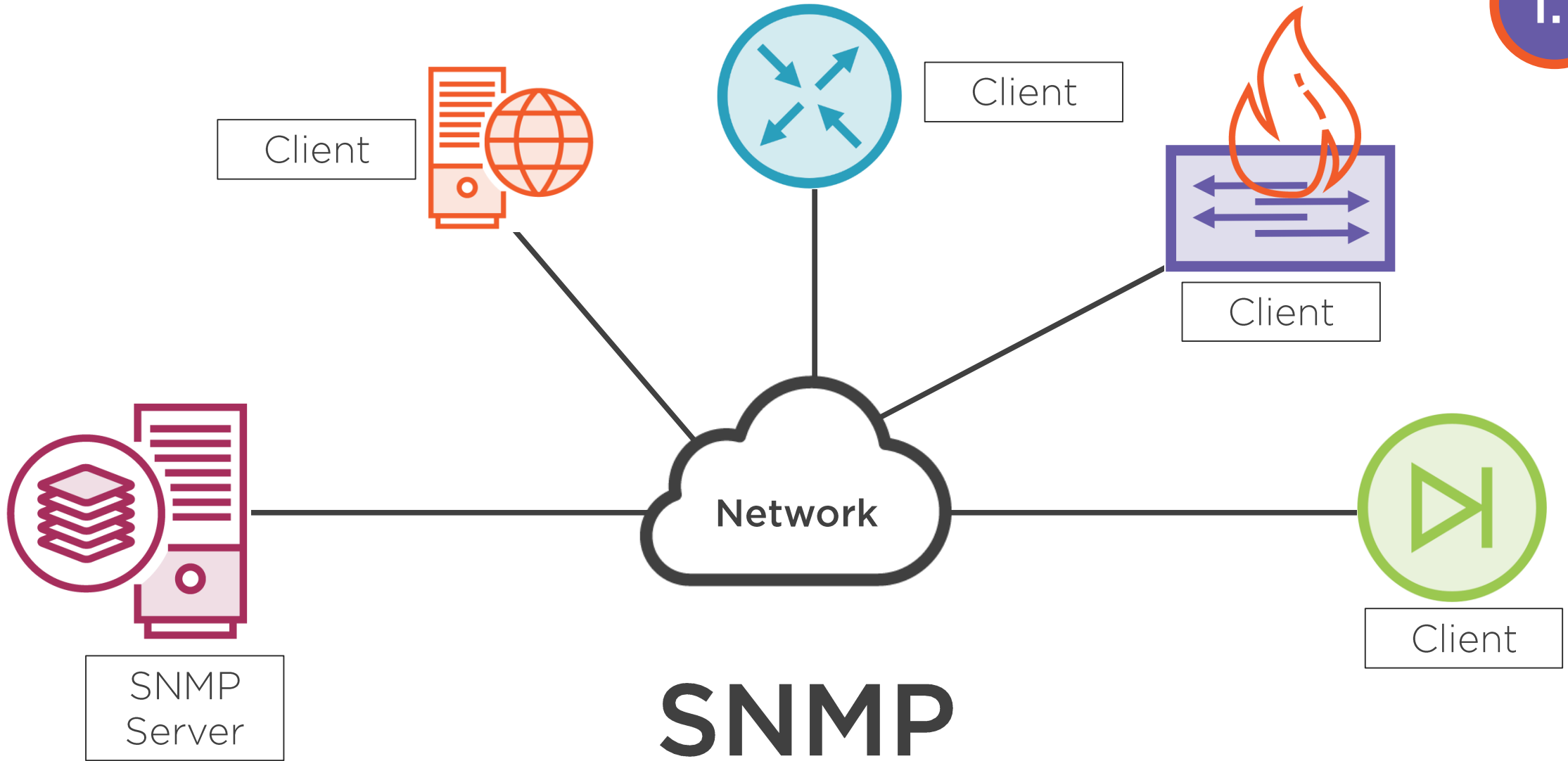


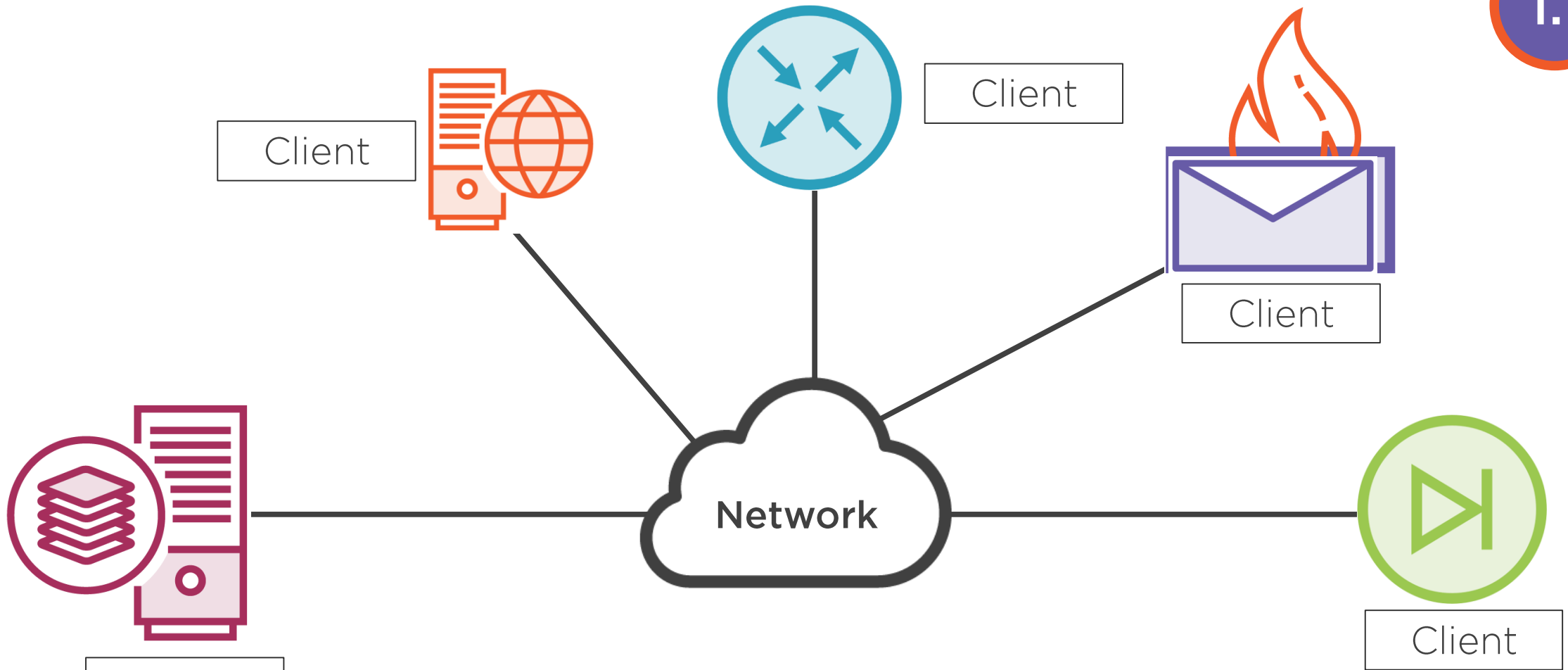


SNMP

“Walk the Tree”

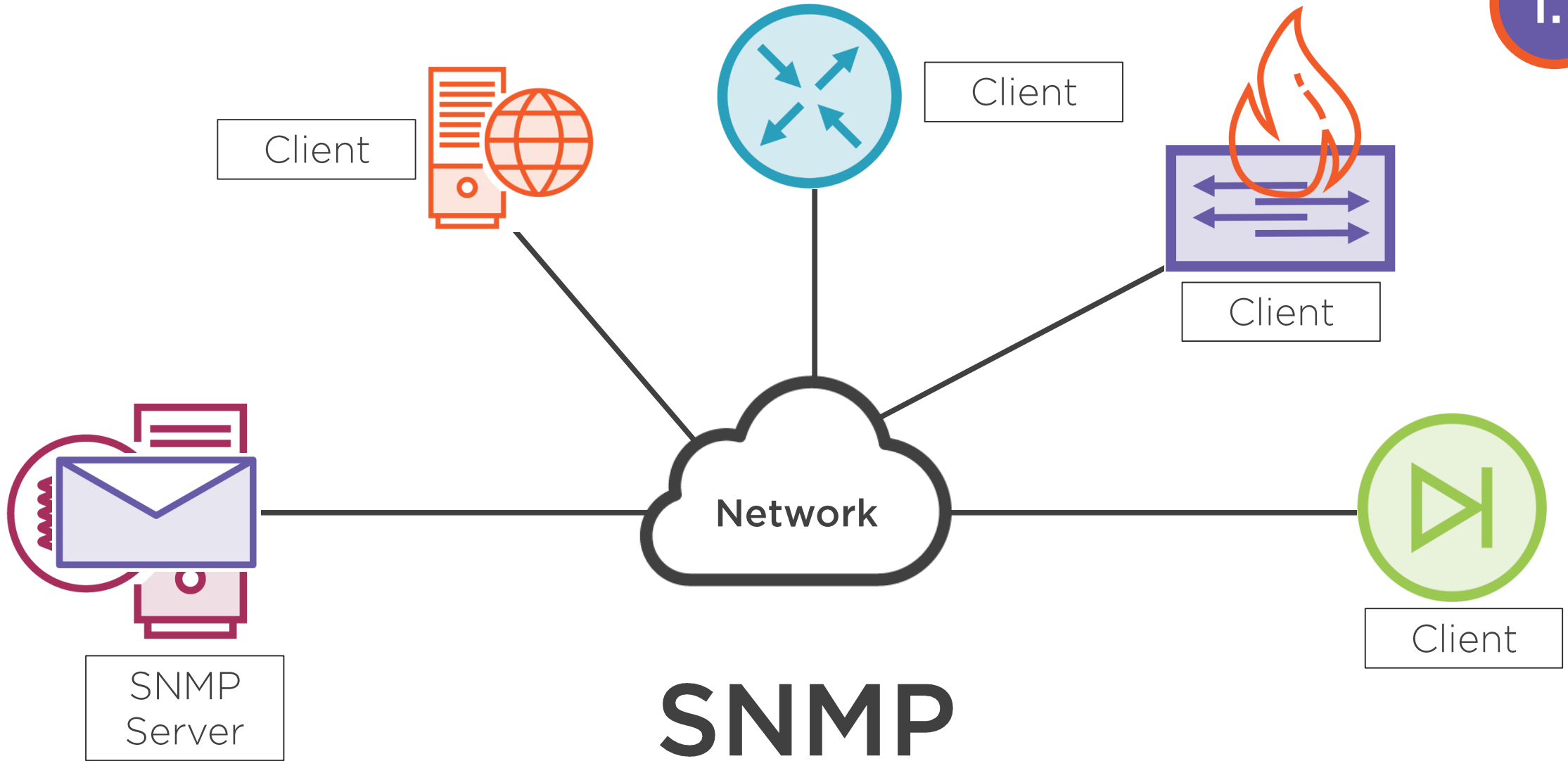






SNMP Trap





Remote Desktop Protocol

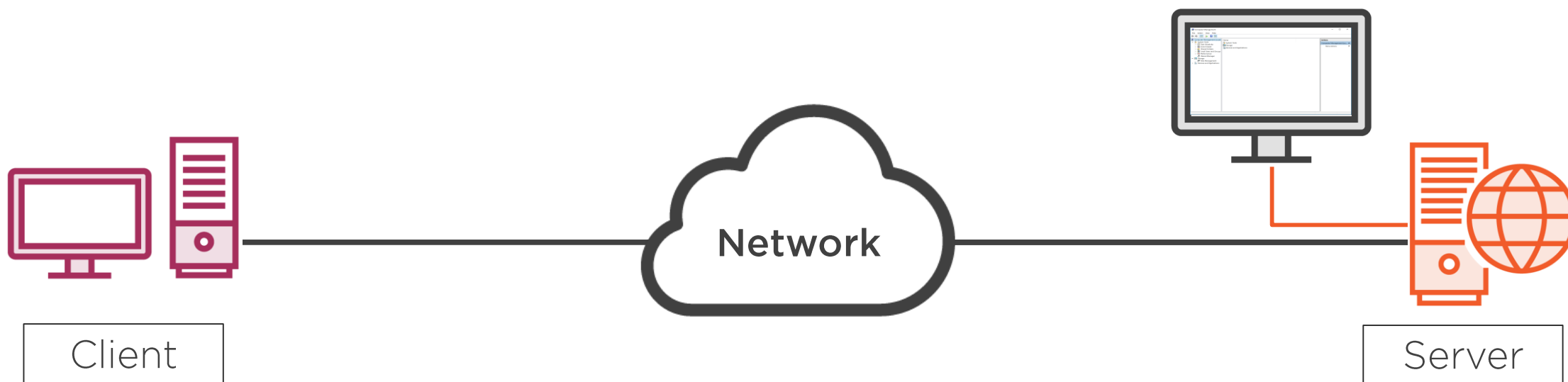
RDP



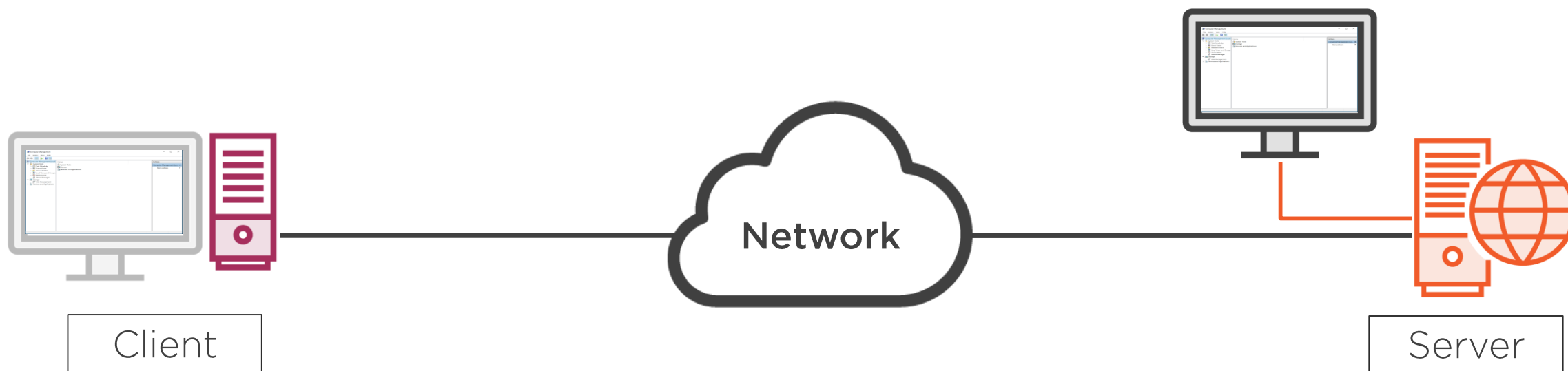
RDP



RDP

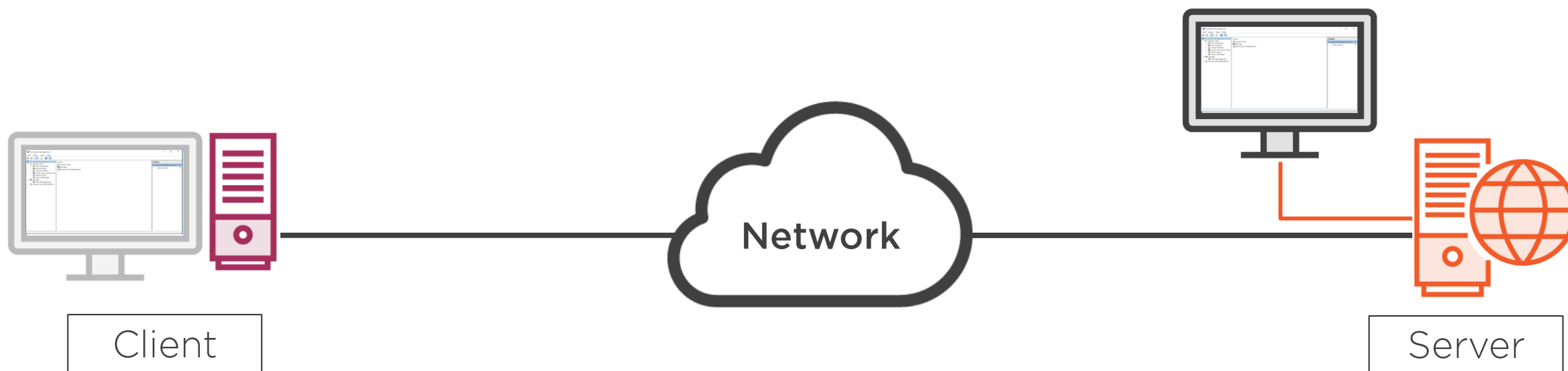


RDP



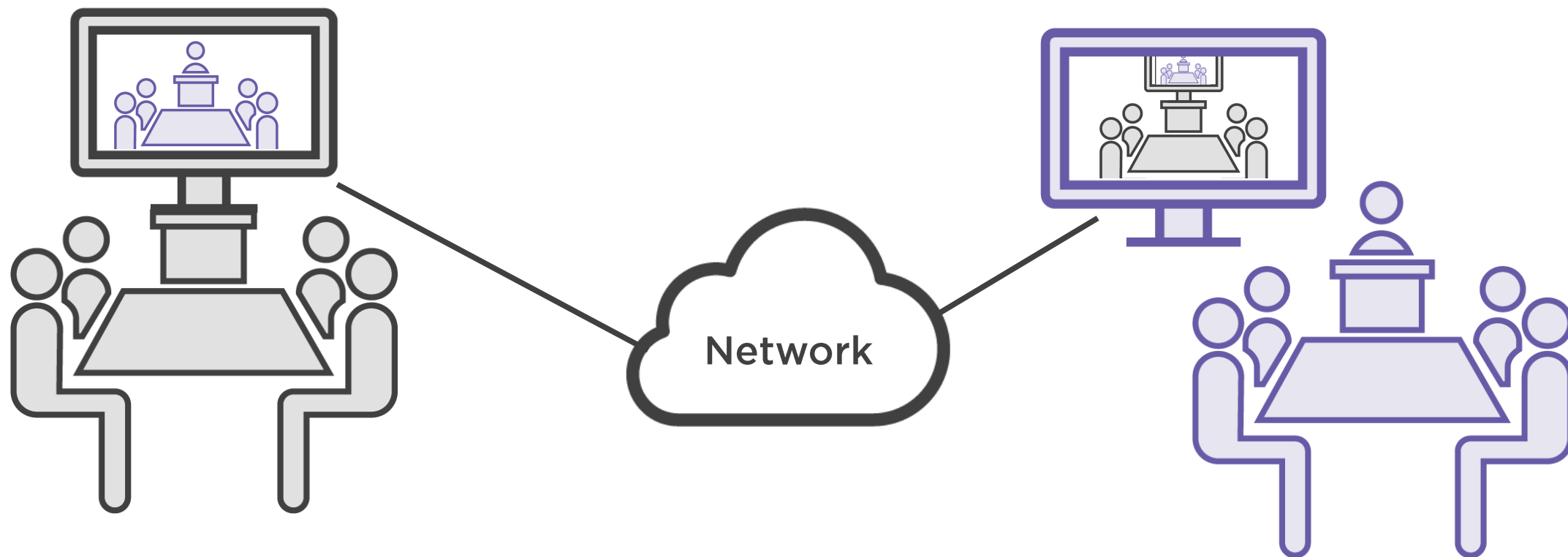
RDP

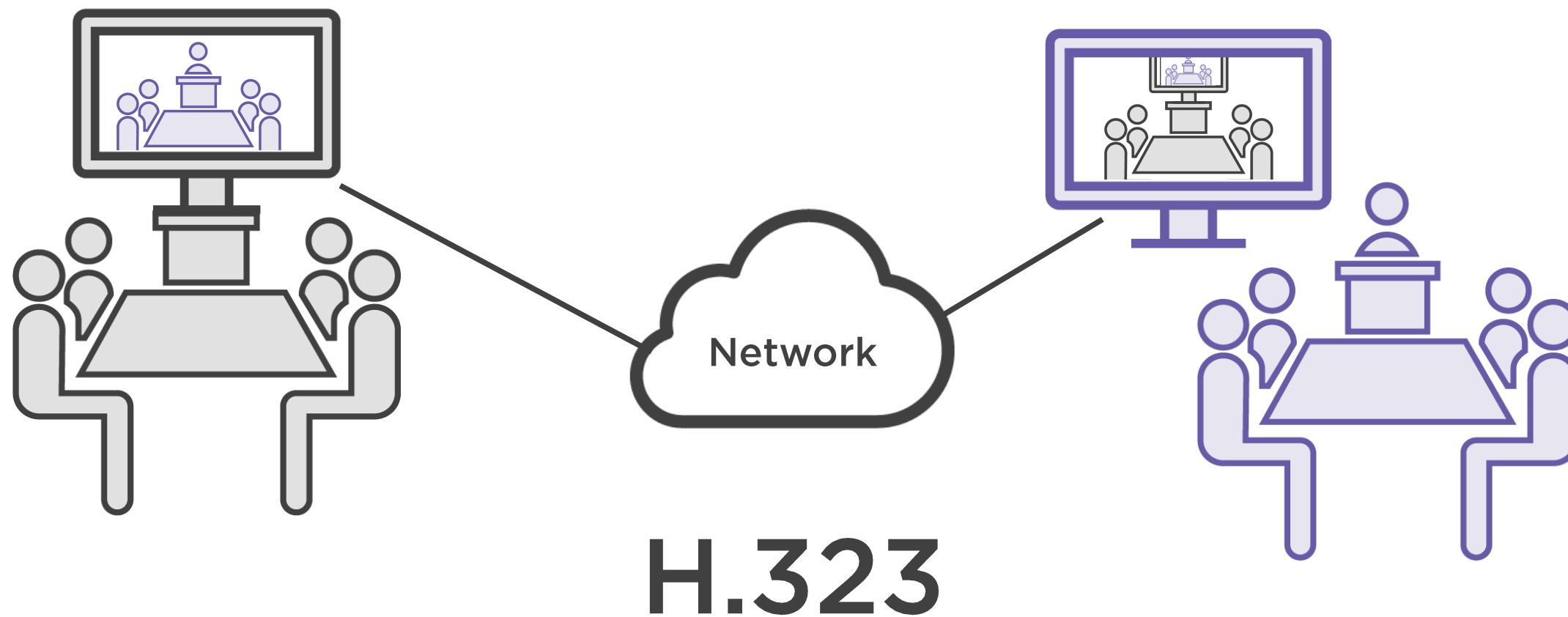
3389

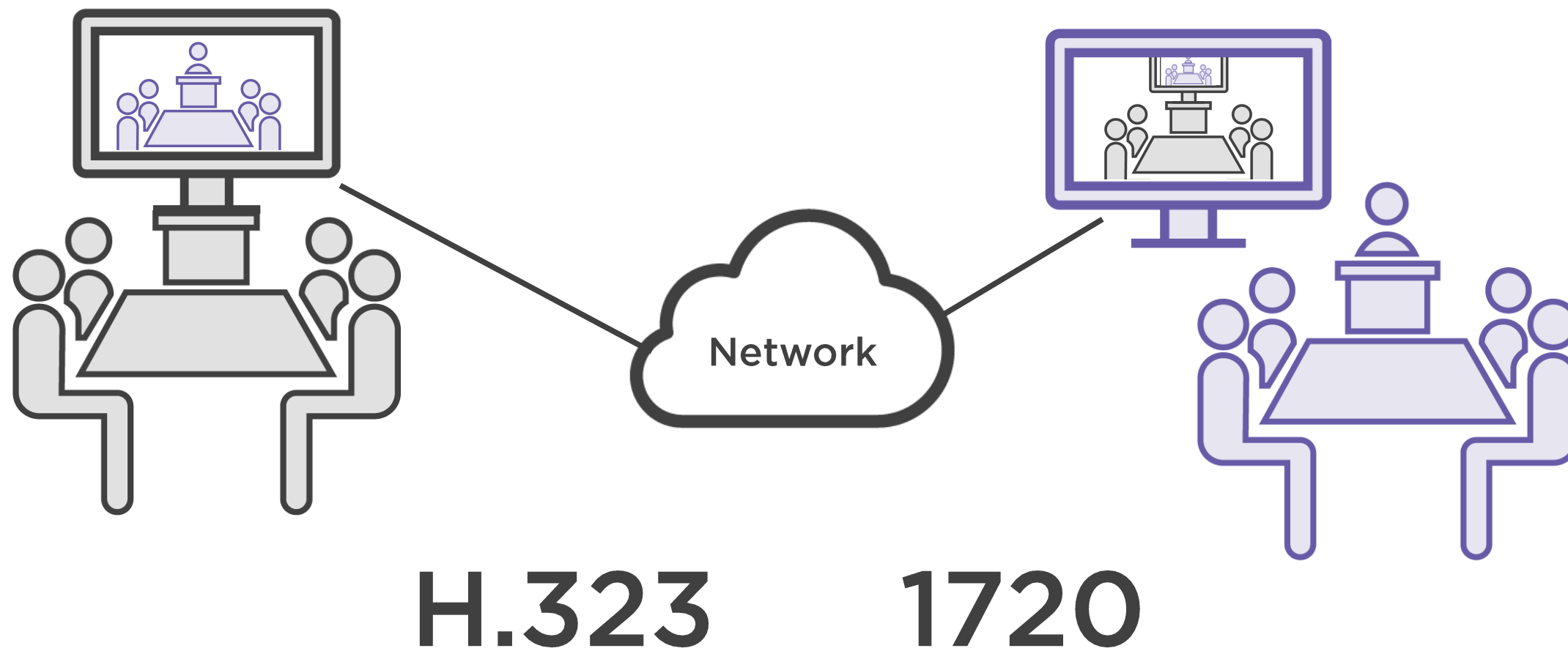


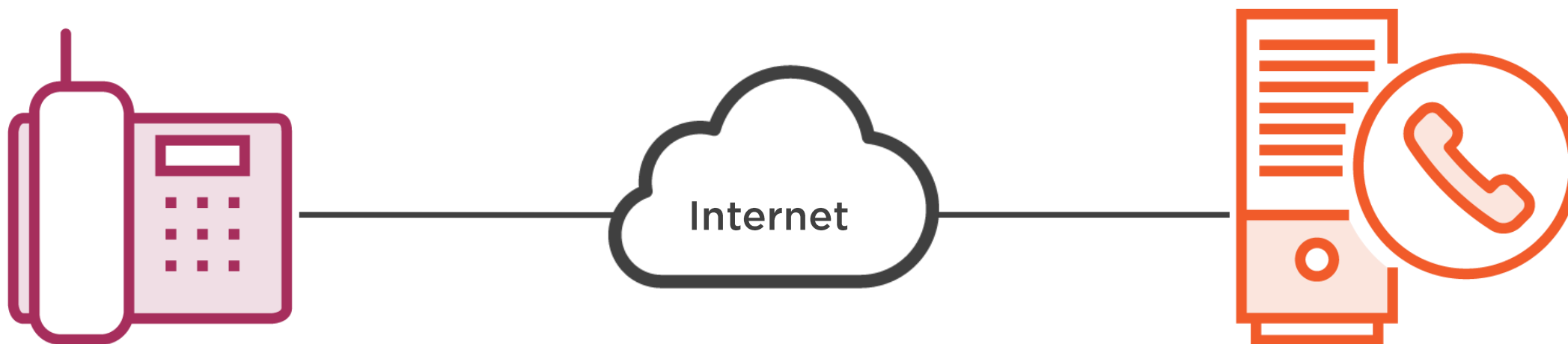
Audio/Visual











SIP

5060 / 5061

Summary



Application Layer Protocols

- Data Transfer Protocols
- Authentication Protocols
- Network Service Protocols
- Network Management Protocols
- Audio/Visual Protocols