W-3, D-3

1. What is the Transport Rule? What are the components of transport Rule?

Mail Flow Rules or **Transport Rules**	✓ Similar to the Inbox rules that are available in Outlook and Outlook on the web. ✓ The main difference is mail flow rules take action on messages while they're in transit, and not after the message is delivered to the mailbox. ✓ Mail flow rules contain a richer set of conditions, actions & exceptions, which provides the flexibility to implement many types of messaging policies.
Components of Transport Rule	✓ **Conditions**: Identify the messages that you want to apply the actions to. If there are no conditions or exceptions, the rule is applied to all messages. ✓ **Actions**: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. ✓ **Exceptions**: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. ✓ **Properties**: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule and the period when the rule is active.

W-3, D-3

2. How to encrypt a message?

When you need to protect the privacy of an email message, encrypt it. Encrypting an email message in Outlook means it's converted from **readable plain text** into **scrambled cipher text**. Only the recipient who has the **private key** that matches the **public key** used to encrypt the message can **decipher** the message for reading. Any recipient without the corresponding private key, however, sees **indecipherable** text. Outlook supports two encryption options:

- ✓ **S/MIME encryption** - To use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard

- ✓ **Microsoft 365 Message Encryption (Information Rights Management)** - To use Microsoft 365 Message Encryption, the sender must have Microsoft 365 Message Encryption, which is included in the **Office 365 Enterprise E3 license.**

Encrypt a Message for Single User from Outlook Client

- ✓ Please open outlook client
- ✓ Please navigate to –
① **New Email** > ② **File** > ③ **Properties** > ④ **Security Settings** > ⑤ Check on - **Encrypt Message Contents & Attachments** > ⑥ press **OK**

Encrypt all Outbound Messages from Outlook Client

- ✓ Please open outlook client
- ✓ Please navigate to – **File** > **Option** > **Trust Center** > **Trust Center Settings** > **Email Security** > Check on – **Encrypt contents & attachments for outgoing messages**

3. How to apply disclaimers?

An Example of Disclaimer	✓ A climate change scientist writing an editorial or opinion piece that involves the topic of climate change may include a disclaimer saying that the opinions are his own and not that of his employer.

- ✓ Please go to – https://outlook.office365.com/ecp
- ✓ Please navigate to – ① **mail flow** > ② **rules** > ③ click "**+**" > ④ **Apply disclaimers**

- ✓ Then –
⑤ type a suitable name
⑥ **Apply the rule if** such as **the sender is located - inside the organization**
⑦ **Do the following** such as **forward the message for approval to** – a mailbox
⑧ **Except if** required.
⑨ Set **Audit this rule with severity level**
At last, **choose a mode for this rule,** Select **Enforce** to turn on the disclaimer immediately, or select **Test without Policy Tips** to put a message in the message tracking log instead of adding the disclaimer.
⑩ Press **Save**

W-3, D-3

4. How to bypass spam filtering? In which scenarios we must bypass EOP filtering?

✓ Please go to – https://outlook.office365.com/ecp

✓ Please navigate to – ① **mail flow** > ② **rules** > ③ click "**+**" > ④ **Bypass spam filtering**

✓ Then –

⑤ **Apply the rule if** such as **the sender is located - inside the organization**

⑥ **Do the following** such as **Set the spam confidence level (SCL) to** – a mailbox

⑦ **Except if** required.

⑧ Set **Audit this rule with severity level**

⑨ At last, **choose a mode for this rule,** Select **Enforce** to turn on immediately, or select **Test without Policy Tips** to put a message in the message tracking log instead of adding the rule.

⑩ Press **Save**

Scenarios to Bypass EOP Filtering

✓ To bypass spam filtering in Office 365 for clean mail that is being sent from any trusted organization or person.

✓ In most cases, email passing through external organizations/persons and then double scanned by Office 365 will cause issues.

✓ Although not critical, in most scenarios, the double scan will result in legitimate emails being dumped into the Outlook junk folder. This can be avoided with a simple bypass filter.

✓ When we are supposed to work with third party webserver in that case mainly bypass filter needs. Like by using the IP allow list you are allowing all email from that web server's IP address to bypass your spam filters. In effect, you're trusting the web hosting company to prevent other customers who are also on the shared hosting server from spamming or phishing your users. It's unlikely that the web hosting company will be able to prevent that. Furthermore, any insecurity in the web form itself could lead to abuse.

✓ So, to enhance your protection without opening yourself up to a new risk, you can use a mail flow rule instead. The mail flow rule is configured to ensure that mail from the web server is still subject to spam filtering if it doesn't have the specific characteristics of the sales contact form emails.

W-3, D-3

5. What is EOP trace?

EOP Trace	
	✓ Offers many different reports that can help to determine the overall status and health of your organization. Some reports are available in the Microsoft 365 admin center, while others are available in the Exchange admin center (EAC).
	✓ The message trace feature in the EAC lets you, as an administrator, follow email messages as they pass through the EOP.
	✓ Helps to determine whether a targeted email message was **received, rejected, deferred**, or **delivered** by the service.
	✓ Shows what **actions** have occurred to the message before reaching its final status.
	✓ **Obtaining detailed information** about a specific message lets you efficiently answer your user's questions, troubleshoot mail flow issues, validate policy changes, and alleviates the need to contact technical support for assistance.

6. How to do message trace in EAC?

✓ Please go to – https://outlook.office365.com/ecp
✓ Please navigate to – **mail flow > message trace**

1. **Date range –** Select **Custom** to get the report

2. **Time zone -** Select your local timezone

3. **Start/End Date & Time -** The difference must be greater than 7 days to get the report (#8 option)

4. **Delivery Status -** Choose any – All, Delivered, Failed, Expanded

5. **Message ID -** Possible to get from MHA

6. **Sender -** Mailbox or wildcard

7. **Recipient -** Mailbox or wildcard

8. **Include message events and routing details with report -** Check this

9. **Report tittle -** Set a suitable report name

10. **Notification email address -** Email address where the report will be sent (inside organization mailbox)

11. Press **Search**

You will see a prompt window that your **message trace has been submitted.** It will take some time to generate the report.

7. What is the accepted domain? Define all type of accepted domains.

Accepted Domain	✓ SMTP name spaces (also known as address spaces) that are configured in an Exchange organization to receive email messages. ✓ For example, my company registered the domain contoso.com, and you configured a mail exchanger (MX) record in your Internet DNS for contoso.com, you need to configure contoso.com as an accepted domain in your Exchange organization to accept messages that are addressed to @contoso.com recipients.

Types of Accepted Domain	✓ **Authoritative domains:**
	  o Recipients (in particular, mailboxes) are configured with email addresses in these domains.
	  o The Exchange organization accepts messages that are addressed to recipients in these domains and is responsible for generating non-delivery reports (also known as NDRs or bounce messages) for non-existent recipients.
	
	✓ **Relay domains:**
	  o The Exchange organization accepts messages that are addressed to recipients in relay domains but aren't responsible for generating NDRs for non-existent recipients.
	  o Instead, Exchange (with additional configuration) relays the messages to messaging servers that are external to the Exchange organization.
	  o Relay domains can be internal (for domains that you control) or external (for domains that you don't control).

8. What is Remote domain? Which features are included in Remote domain?

	✓ **Organizational setting** that allows controlling certain message types such as "Out of Office" and "Non-Delivery Reports".
	✓ In 4 cases we may need a remote domain –
	  i. Don't allow to forward messages to recipients in other domains.
	  ii. You work with an organization that you don't want to receive automatic messages.
	  iii. You have a business partner that's outside your organization, and you'd like that partner to receive the same out-of-office replies as those received by people inside your organization.
	  iv. Your users frequently send email to a company that supports limited email formats, and you'd like to make sure all emails sent to that organization are sent in a format that they can read.

Features in Remote Domain	✓ Out-of-office messages ✓ Automatic replies ✓ Automatic forwards ✓ Delivery reports ✓ Non-delivery report ✓ Meeting forward notifications

9. What do connectors do? How to set up a connector?

Connector	✓ **Collection of instructions** that customize the way your **email flows to and from** your Microsoft 365 or Office 365 organization. ✓ Most Microsoft 365 and Office 365 organizations don't need connectors for regular mail flow. ✓ Only necessary for the hybrid environment.
Set up Connector	We need connectors for 4 scenarios – i. Standalone EOP subscription. ii. Some of the mailboxes are on on-premises email servers, and some are in Exchange Online. iii. All of the mailboxes are in Exchange Online, but you need to send email from sources in your on-premises organization. iv. You frequently exchange sensitive information with business partners, and you want to apply security restrictions. These 4 options are available to set up connectors (**From & To**) - ✓ Office 365 ✓ Your Organization Email Server ✓ Partner Organization ✓ Internet

10. How old and recent message can be traced?

- ✓ Messages less than 4 hours old might not be available.
- ✓ Messages older than 90 days are unavailable.

11. When mail flow works?

Before delivered to user mailbox in EOP stage.

W-3, D-3

12. Explain the features of mail flow.

<table>
<tr><td rowspan="7">Mail Flow

(RuMU ARC)</td><td>Rules</td><td>✓ Apply disclaimers
✓ Bypass filter
✓ Restrict messages by sender or recipient
✓ …………………………</td><td>✓ Apply this rule if
✓ Do the following
✓ Except if

✓ Audit this rule with severity level
✓ Choose a mode for this rule
✓ Stop Processing more rules
✓ …………………………………………</td></tr>
<tr><td rowspan="11">Message trace</td><td>Date Range</td><td>o Past 48 hours (summary trace)
o Past 24 hours (summary trace)
o Past 7 days (summary trace)
o Custom (only for EOP trace)</td></tr>
<tr><td>Time zone</td><td></td></tr>
<tr><td>Start/End Date & Time</td><td></td></tr>
<tr><td>Delivery Status</td><td>o All
o Delivered
o Failed
o Expanded</td></tr>
<tr><td>Message ID</td><td></td></tr>
<tr><td>Recipient</td><td></td></tr>
<tr><td>Sender</td><td></td></tr>
<tr><td colspan="2">(only Activate when duration is more than 7 days & date range set custom)</td></tr>
<tr><td>✓ Include message events & routing details with report (looking for a small number of messages)</td><td></td></tr>
<tr><td>Direction</td><td>o All
o Inbound
o Outbound</td></tr>
<tr><td>Report title</td><td></td></tr>
<tr><td>URL trace</td><td></td><td></td></tr>
<tr><td>Accepted domains</td><td></td><td></td></tr>
<tr><td>Remote domains</td><td>Default</td><td>✓ Out of Office automatic replies
✓ Automatic replies
✓ Automatic Forwarding
✓ Delivery report
✓ Non-delivery report
✓ Meeting Forward Notification</td></tr>
<tr><td>Connectors</td><td>✓ From
✓ To</td><td>✓ Office 365
✓ Your Organization's email server
✓ Partner Organization
✓ Internet</td></tr>
</table>

Note: The "Message trace" section also includes a row "Notification email address" following "Report title".