W-3, D-5

1. What is SMTP/POP3/MAPI/IMAP/ActiveSync/Autodiscover?

SMTP	✓ **Simple Mail Transfer Protocol** (SMTP) is the standard protocol for sending emails across the Internet. ✓ Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. ✓ SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.
POP3	✓ **Post Office Protocol version** 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. ✓ POP3 allows you to download email messages on your local computer and read them even when you are offline. ✓ Messages are downloaded locally and removed from the email server.
MAPI	✓ MAPI stands for **Messaging Application Programming Interface**. ✓ MAPI is a proprietary Microsoft protocol that allows the Microsoft Outlook email client to fully utilize all of the features of an Exchange server including email, shared address books, calendars and public folders. ✓ When Outlook is configured as a MAPI client, also known as an Exchange client, email is stored in the cloud on Comcast's secure mail server with a copy on your computer. ✓ Messages retained in the cloud are accessible via webmail from any internet connected computer. ✓ With MAPI, you can move messages from the cloud into a local file on your computer called a .PST file, a process through which copies of messages are deleted from the cloud and stored on your computer.
IMAP	✓ The **Internet Message Access Protocol** (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. ✓ IMAP is the most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers. ✓ IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.
ActiveSync	✓ Exchange ActiveSync is a proprietary protocol that syncs your mobile device with your Exchange mailbox, so you can access your email, calendar, contacts, tasks, and so much more. ✓ It is based on XML and communicates with a mobile device using HTTP or HTTPS.

W-3, D-5

Autodiscover	✓ Autodiscover is the feature that Outlook uses to obtain configuration information for servers to which it connects. ✓ Kind of DNS records (CNAME). ✓ Help us to configure email client.

2. What are the steps of Autodiscover? How to check Autodiscover?

1) **SCP Lookup**:
   - ✓ SCP refers to **Service Connection Point**, which the clients of the service use the data in an SCP to locate, connect to, and authenticate an instance of your service.
   - ✓ **SCP data return a path of the Autodiscover XML.**
   - ✓ An attempt is then made to each URL that's returned by the SCP lookup to try to retrieve the Autodiscover payload.
   - ✓ If fails to retrieve the payload, it is moved to root domain query.

2) **HTTPS root domain query**:
   - ✓ In this step, Outlook builds a URL from the domain name of the initial address in the format of **https://<domain>/autodiscover/autodiscover.xml** and tries to retrieve the payload from the resulting URL.
   - ✓ Because many root domains aren't configured for Autodiscover, Outlook purposefully silences any certificate errors that occur during the attempted retrieval.
   - ✓ If this step doesn't acquire the payload, it is moved to the next step.

3) **HTTPS Autodiscover domain query**:
   - ✓ In this step, Outlook create a URL from the domain name of the initial address in the format of **https://autodiscover.<domain>/autodiscover/autodiscover.xml** and tries to retrieve the payload from the resulting URL.
   - ✓ Since it's a primary URL typically for Autodiscover data, it doesn't silence any certificate errors that occur during the attempted retrieval.
   - ✓ If this step doesn't acquire the payload, it is moved to the next step.

4) **Check for local XML file:**
   - ✓ In this step Outlook will check the local XML file, whether the file is found or not.
   - ✓ If the payload is not retrieved, it is moved to the next step.

5) **HTTP Redirect Method:**
   - ✓ In this step, outlook sends a request to the Autodiscover domain URL **http://autodiscover.<domain>/autodiscover/autodiscover.xml** and test for redirect responses.
   - ✓ If an actual Autodiscover XML payload is returned and not a redirect, Outlook ignores the actual Autodiscover XML response because it was retrieved without the http security.
   - ✓ If it's a valid redirect URL, Outlook follows the redirect and will try to retrieve a payload XML from the new URL.

W-3, D-5

- ✓ Outlook will also look for harmful URL's in this step.
- ✓ If the payload is not retrieved, it is moved to the next step.

6) **SRV Record query:**
   - ✓ In this step, Outlook will perform a DNS inquiry and it will check for the for the first record that uses https as its protocol.
   - ✓ Then it tries to retrieve the payload from that URL.
   - ✓ If the payload is not retrieved, it is moved to the next step.

7) **Cached URL in the Outlook profile:**
   - ✓ In this step, outlook will check for the cached URL in the Outlook profile.
   - ✓ This step is performed by the Outlook itself, if it finds any cached it will retrieve the payload
   - ✓ If not then it is moved to the next step.

8) **Direct Connect to Office 365:**
   - ✓ If Autodiscover is working and pointing to the correct server, Outlook should use it to find the mail server, so verify that it is working.
   - ✓ Use the Remote Connectivity Analyzer to check your records.
   - ✓ If Outlook is unable to reach Autodiscover, Outlook will attempt to find your mail server using the method Direct Connect.

How to Check Auto Autodiscover through Outlook Client

- ✓ Please open Outlook client
- ✓ Click on the show hidden icons > press and hold down the **CTRL** key, and then right-click the Outlook icon in the system tray.
- ✓ A menu will appear and select **Test E-mail AutoConfiguration**
- ✓ Use Autodiscover should be checked by default. You can also check and uncheck the other options Use Guesscheck and Secure Guessmart Authentication checkboxes.
- ✓ Provide your email address and passwords and click on Test.
- ✓ The Result tab shows that the Autodiscover is detected. You can also check for log and XML details by clicking the tabs.

How to Check Auto Autodiscover through Email Connectivity Analyser

- ✓ Please go to - https://testconnectivity.microsoft.com/
- ✓ Click on **Outlook Connectivity**
- ✓ A new window will appear. Provide the **Email address**, Microsoft account and **Password**.
- ✓ Click on **Use Autodiscover** to detect server settings and check on the terms.
- ✓ Then provide the captcha for verification and finally click on Perform Test.

W-3, D-5

3. What is the purpose of Autodiscover?

Purpose of Autodiscover	✓ Helps to configure Email client ✓ Synchronize outlook client to Exchange Sync ✓ Free/Busy information in your calendar ✓ Out of office automatic response messages setup in Outlook. ✓ Proper syncing of Offline Address Book ✓ Folder Sharing with sending out the Sharing invitation.

4. Test Autodiscover from https://testconnectivity.Microsoft.com/ and read the generated report.

- ✓ Please go to - https://testconnectivity.microsoft.com/
- ✓ Click on **Outlook Connectivity**
- ✓ A new window will appear. Provide the **Email address**, Microsoft account and **Password**.
- ✓ Click on **Use Autodiscover** to detect server settings and check on the terms.
- ✓ Then provide the captcha for verification and finally click on Perform Test.

5. What is SMTP Relay?

SMTP Relay	✓ SMTP relay let office 365 replays emails on behalf of you by using a connector. ✓ Configured with public IP address or a TLS certificate. ✓ Any email address including Office 365 mailboxes can send mail using an SMTP relay, as long as it uses a domain that is set up as your in-office 365 ✓ Possible to use multi-factor authentication (MFA). ✓ Possible to send email to external recipients

6. Why do we need SMTP relay?

- ✓ An SMTP relay service is the best way to manage **batch sends** and **automated emails**.
- ✓ Sending over SMTP through a trusted 3rd party will help you ensure that you don't experience **deliverability issues** and that your mail keeps flowing to the inbox without any issues.

W-3, D-5

7. What is the limitation of accessing email account through POP3, IMAP?

Limitation of Accessing email through POP3	✓ Multiple connection using same email address is not possible. ✓ POP3 stores the email on the local storage of the client. ✓ POP3 clients remove downloaded messages from the email server. ✓ Difficult to access email on multiple computers. ✓ POP3 can't synchronize multiple folders on the email server with multiple folders on the client computer. ✓ POP3 also doesn't support public folder access.
Limitation of Accessing email through IMAP	✓ Multiple connection is possible using same email address (20 connections per IP address).
Common Limitation	✓ For always-connected clients, the user might **configure the email application** to send and receive messages every set number of minutes. ✓ Each time opening Microsoft 365 email, user will experience a **delay** of several seconds. ✓ **Modern Authentication** will not work for legacy protocols, such as POP3 and IMAP4. ✓ Don't offer **rich email**, **calendaring**, and **contact management**, or other features that are available when users connect with Outlook, Exchange ActiveSync, Outlook on the web

8. Why do we SMTP?

- ✓ SMTP is used to **send emails**, so it only works for **outgoing emails**.
- ✓ To be able to send emails, you need to provide the correct SMTP server when you set up your email client.
- ✓ Unlike POP3 and IMAP, SMTP can't be used to retrieve and store emails.
- ✓ SMTP is also responsible for setting up communication between servers.

9. How to enable Autodiscover?

- ✓ MS Admin > Settings > Domain > DNS Records > Add
- ✓ From Domain Hosting Provider, DNS Management

W-3, D-5

10. What are the methods to send mail using Microsoft 365? Know the differences of each methods

There are three methods to send mail using Microsoft 365:

	(1) SMTP client submission	(2) Direct send	(3) SMTP relay
Features			
MFA	No	Uses	uses
Send to recipients in your domain(s)	Yes	yes	yes
Relay to internet via Microsoft 365	Yes.	No. Direct delivery only	yes
Bypasses antispam	Yes, if the mail is destined for one of your Microsoft 365 or Office 365 mailboxes	No. Suspicious emails might be filtered. We recommend a custom Sender Policy Framework (SPF) record.	No. Suspicious emails might be filtered. We recommend a custom SPF record. Redirect to HRDP
Supports mail sent from applications hosted by a third party	Yes	Yes. We recommend updating your SPF record to allow the third party to send as your domain	No
Saves to Sent Items folder	Yes	No	No
Requirements			
Open network port	Port 587 or port 25	Port 25	Port 25
Device or application server must support TLS	Required (1.2 & above)	Optional	Optional
Requires authentication	Microsoft 365 or Office 365 username and password required	None	One or more static IP addresses.
Limitations			
Throttling limits	10,000 recipients per day. 30 messages per minute.	Standard throttling is in place to protect Microsoft 365 or Office 365 Throttling limits	Reasonable limits are imposed. The service can't be used to send spam or bulk mail.

W-3, D-5

11. What are the different methods to configure SMTP Relay?

Configured with IP address-based connector	✓ Obtain the public (static) IP address that the device or application with send from. ✓ A dynamic IP address isn't supported or allowed. ✓ You can share your static IP address with other devices and users, but don't share the IP address with anyone outside of your company.
Configured with TLS Certificate based connector	✓ Verify the subject name on the certificate used by the sending device or application. ✓ The common name (CN) or subject alternative name (SAN) in the certificate should contain a domain name that you have registered in Microsoft 365 or Office 365. ✓ Must create a certificate-based connector in Microsoft 365 or Office 365 with this same domain name to accept and relay emails coming from these devices, applications, or any other on-premises server.