# Tìm hiểu về các công nghệ mạng 1G, 2G, 3G, 4G,5G

1G ( Thế Hệ 1)

Được giới thiệu vào những năm 19801G là công nghệ không dây viễn thông thương mại đầu tiên. Lần đầu tiên, Điện thoại và Điện thoại Nippon (NTT) đã giới thiệu nó ở Tokyo, Nhật Bản. Từ đó, nó nhận được sự chú ý của người tiêu dùng và chiếm thị phần lớn. Năm 1981, 1G được giới thiệu ở một số nước châu Âu và năm 1983; 1G thâm nhập vào thị trường Mỹ.

Công nghệ: 1G sử dụng tín hiệu vô tuyến tương tự để liên lạc.

Tốc độ: Tốc độ 1G chỉ đơn thuần lên tới 2,4Kb / giây.

Chức năng: 1G chỉ có thể được sử dụng cho các cuộc gọi thoại.

Tính linh hoạt: Trước đó, điện thoại yêu cầu kết nối có dây để liên lạc. Sau sự phát triển này, mọi người hoàn toàn có thể mang điện thoại ra ngoài trời với mạng 1G.

Thay thế: 1G thay thế thành công các công nghệ vô tuyến 0G, chẳng hạn như Hệ thống điện thoại di động (MTS), Hệ thống điện thoại di động tiên tiến (AMTS) và Push to Talk (PTT), chiếm ưu thế trong những ngày đó.

2G (Thế Hệ 2 )

Vào năm 1991 tại Phần Lan, sự phát triển của công nghệ đã có một bước ngoặt mới và một thế hệ mới 2G. 2G được dựa trên tiêu chuẩn GSM. Công nghệ này dường như đã biến 1G trở nên lỗi thời và có sự tiên tiến hơn nhiều.

Có gì mới: Công nghệ 2G cho phép người dùng gửi và nhận tin nhắn văn bản và tin nhắn đa phương tiện (MMS).

Công nghệ: 2G sử dụng tín hiệu số để liên lạc với tháp radio.

Tốc độ: Tốc độ truyền của Mạng 2G tăng lên nhiều lần và đạt tốc độ truyền tối đa theo lý thuyết là 50Kb / giây với sự trợ giúp của Dịch vụ vô tuyến gói chung (GPRS).

Năng lượng pin: 2G yêu cầu năng lượng pin thấp do mức tiêu thụ pin thấp bởi tín hiệu kỹ thuật số.

Chất lượng: Chất lượng âm thanh được cải thiện và người dùng không phải đối mặt với bất kỳ tiếng ồn nền nào.

Quyền riêng tư: 2G đã cải thiện quyền riêng tư của người dùng vì các tin nhắn và MMS được mã hóa kỹ thuật số và chúng chỉ được mở đối với người dùng mà thôi.

Không còn thiết bị cầm tay nhân bản: Trong thời của 1G, có thể sở hữu hai thiết bị cầm tay có cùng số. Nhưng, 2G đã khép lại chương này và chấm dứt mọi cơ hội có hành vi gian lận liên quan đến hai con số.

Nhược điểm:

• Âm thanh giảm : Nó xảy ra trên tài khoản của việc sử dụng nén mất dữ liệu bởi các mã.

3G (Thế Hệ Thứ 3)

Về mọi mặt dịch vụ thì 3G là thế hệ tiếp theo. 3G được giới thiệu vào năm 2001 và tuân theo các tiêu chuẩn do Liên minh Viễn thông Quốc tế (ITU) đặt ra.

Tốc độ truyền: 3G cung cấp tốc độ internet nhanh nhưng phụ thuộc vào công nghệ được sử dụng bởi nhà cung cấp.

• 144Kbps-2Mbps

• WCDMA = 384Kb / giây

• HSPA hoặc 3.5G = 7.2Mbps

• HSPA + hoặc 3,75G = 21,6 Mb / giây

Mang lại một cuộc cách mạng [công nghệ](https://ampedgaming.com/cong-nghe/): khái niệm sử dụng điện thoại di động thì 3G đã thay đổi hoàn toàn. Các ứng dụng di động khác nhau như Whatsapp, IMO, có thể được sử dụng cho các cuộc gọi thoại và video trên toàn thế giới. Từ chiếc điện thoại đi động của mình thì bạn hoàn toàn có thể sử dụng truyền dữ liệu một cách nhanh chóng.

Ứng dụng: GPS, Truyền hình di động, Video theo yêu cầu, Hội nghị video.

Chi phí dịch vụ: Mặc dù việc sử dụng 3G có thể tiêu tốn một khoản tiền lớn, thế nhưng bạn vẫn có thể lựa chọn những dữ liệu phù hợp cùng với các nhà mạng có sẵn.

4G (Thế Hệ Thứ 4)

4G là công nghệ tiên tiến và nâng cấp nhất hiện nay. 4G là phiên bản cải tiến của 3G. 4G có sẵn ở hai dạng là WiMAX (Khả năng tương tác toàn cầu để truy cập vi sóng) và LTE (Tiến hóa dài hạn). Phiên bản LTE của 4G được sử dụng rộng rãi và hầu hết có sẵn.

Tốc độ:

• Đầu năm 2008, ITU đưa ra các tiêu chuẩn cho 4G, theo Nâng cao Viễn thông di động quốc tế (IMT-Advanced) và đặt tốc độ tối thiểu ở mức 100 Mbps và tối đa 1Gbps. Kết nối cung cấp tốc độ truyền này có thể được đặt tên là 4G.

• Nói cách khác, ở vị trí đứng yên, tốc độ phải ở khoảng 1 Gbps và trong khi di chuyển phải tối thiểu 100 Mbps.

Ứng dụng: TV HD, HD VOD, TV 3D và Trò chơi.

5G (thế hệ thứ 5)

5G được thảo luận nhiều về thế hệ tiếp theo và có thể nhanh hơn nhiều lần so với 4G ngày nay. Công nghệ 5G đang được thử nghiệm trong các phòng thí nghiệm và chỉ được chạy trên cơ sở thử nghiệm.

Các ứng dụng có thể: Thực tế tăng cường, Thực tế ảo, Xe tự lái.

Công nghệ có thể: Công nghệ chính được sử dụng có thể là các dải sóng Millimet hoạt động ở dải tần 30 GHz đến 300 GHz. Băng tần hiện đại, được sử dụng bởi các nhà cung cấp mạng là dưới 6 GHz.

Tốc độ dự kiến: Tốc độ tải xuống và tải lên có thể lần lượt là khoảng 20 Gbps và 10 Gbps .

1. Công nghệ 1G là gì?

Đây là thế hệ mạng đầu tiên của mạng di động viễn thông với kết nối analog. Được giới thiệu lần đầu tiên vào những năm 80 của thế kỉ 20. Mạng 1G hoạt động là nhờ sử dụng công nghệ truyền nhận thông tin thông qua tín hiệu analog.

Năm 1979, mạng di động 1G lần đầu tiên được triển khai thương mại tại Nhật Bản bởi nhà mạng Nippon Telegraph and Telephone (NTT).

Công nghệ 1G chỉ có thể cung cấp được chức năng cơ bản của điện thoại di động là nghe và gọi thoại. Kết nối Analog thì lại rất dễ bị ảnh hưởng bởi thời tiết, do vậy mạng 1G hoạt động tương đối chậm và không ổn định.

Tuy nhiên, sự ra đời của mạng 1G là một bước ngoặt lớn về sự phát triển của công nghệ. Do vậy, kể từ khi ra mắt đến thời điểm 5 năm sau, Nhật Bản trở thành quốc gia đầu tiên phủ sóng 1G trên toàn quốc.

Vào năm 1981, các nước ở khu vực Bắc Âu như Đan Mạch, Phần Lan, Na Uy và Thụy Điển đã triển khai mạng 1G với hệ thống NMT, điểm đặc biệt của NMT là nó có khả năng chuyển vùng.

Tiếp đến là các Quốc gia như Mỹ, Anh, Mexico, Canada đều triển khai mạng di động 1G.

2. Công nghệ 2G là gì?

2G là thế hệ thứ hai của hệ thống mạng di động, được ra mắt đầu tiên vào năm 1992. Mạng 2G nhanh chóng phổ biến và được triển khai thương mại ở Phần Lan bởi nhà mạng Radiolinja.

So với mạng 1G, hệ thống mạng 2G đem tới nhiều những tính năng và tiện ích nổi trội hơn, phải kế đến:

Độ bảo mật thông tin cao: mạng 2G cho phép người dùng gọi thoại với tín hiệu được mã hóa dưới dạng tín hiệu kỹ thuật số (dạng nhị phân 0 và 1). Do vậy, tránh rò rỉ thông tin người dùng.

Tốc dộ dữ liệu đươc cải thiện: Tốc độ dữ liệu đạt 64 Kbps/giây, cao hơn nhiều so với 1G.

Thiết kế nhỏ gọn: Thiết kế có phần nhỏ gọn hơn nhiều so với thế hệ trước. Do được chuyển từ kết nối Analog sang Digital.

Tiện lợi: 2G cũng hỗ trợ nhiều người dùng cùng một lúc trên mỗi dải tần hoạt động.

Hỗ trợ gửi và nhận tin nhắn văn bản SMS.

Ngoài ra, thế hệ mạng 2G còn có 2 phiên bản nữa là mạng 2.5G và mạng 2.75G

Mạng 2.5G: ra mắt vào năm 2000. Đây là phiên bản được nâng cấp cuộc gọi, tin nhắn và kết nối Internet đang dần được hình thành. Tuy nhiên, tốc độ mạng tối đa 50 Kbps. nên việc truy cập Internet là tương đối khó khăn.

Mạng 2.75G: ra mắt năm 2003. Bản này thì chất lượng mạng đã được cải tiến tốt hơn khá nhiều so với mạng GPRS. Tốc độ mạng có thể đạt 1Mbps. Do vậy, việc truy cập Internet để đọc báo đã dễ thở hơn rất nhiều.

Mạng 2.5G (GPRS)

3. Công nghệ 3G là gì?

Đây là thế hệ mạng thứ ba được giới thiệu vào năm 2001 bởi  nhà mạng NTT Docomo. Đến năm 2003, nó đã được thương mại hóa và được phép truyền tải dữ liệu thoại và cả những dữ liệu khác (email, hình ảnh, âm thanh, vide,…). Sự ra đời của mạng 3G đã nhanh chóng thay thế 2G và dần phổ biến ở các nước phát triển.

Sự đột phá của mạng 3G có thể kể đến là tốc độ truyền dữ liệu. Với thông số kết nối từ 384 Kbps đến 2 Mbps/giây, 3G giúp người dùng có thế gửi và nhận mail với tốc độ nhanh chóng.

Mạng 3g có tốc độ mạng cao nhất là HSPA+ (kí hiệu H+) với tốc độ lên đến 42 Mbps. Công nghệ này đã nhanh chóng đáp ứng những nhu cầu giải trí của người dùng.

4. Công nghệ 4G là gì?

Ở thời điểm hiện tại, thế hệ mạng thứ 4 (4G) được sử dụng vô cùng rộng rãi. Ra đời vào năm 2013, 4G cho tốc độ truyền tải dữ liệu cực nhanh. Với tốc độ lý tưởng nhất vào khoản 1Gb đến 1,5Gb trong một giây.

Đặc biệt, 4G LTE được xem là tiêu chuẩn cho các thiết bị công nghệ hiện đại vì tốc độ truyền dữ liệu rất cao, có thể lên tới 12,5MB khi đang di chuyển và thậm chí là cao hơn khi đứng yên.

Mạng 4G không chỉ cung cấp những tính năng nâng cao trải nhiệm người dùng như xem phim, nghe nhạc trực tuyến mà còn nhiều tiện ích khác như chơi game online, xem youtube mà không lo tốc độ mạng bị chậm.

5. Công nghệ mạng 5G là gì?

5G là thế hệ mạng thứ 5 và mới được triển khia trong khoảng 1-2 năm gần đây. Tuy nhiên, 5G còn chưa được phổ cập rộng rãi tới người dùng. Bởi lẽ chi phí triển khai khá cao và chưa có nhiều thiết bị hỗ trợ mạng 5G.

Sự ra đợi của 5G được coi là một cuộc cách mạng trong lĩnh vực công nghệ điện tử. Đây cũng được xem là chìa khóa mở cửa tương lai của con người.

Mạng 5G có tôc độ truyền tải dữ liệu lớn hơn gấp 10 lần 4G. Như vậy, trong điều kiện lý tưởng, 5G có thể truyền tải dữ liệu lên đến 10GB trong một giây. Với tốc độ như thế này, người dùng có thể tải bộ phim dài 2 giờ chưa được 10 giây.

## **Tìm hiểu các chuẩn WLAN IEEE 802.11**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tiêu chuẩn | 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac | 802.11ac-wave1 | 802.11ac-wave2 | 802.11ad |
| Năm phát hành | 1999 | 1999 | 2003 | 2009 | 2013 | 2014 | 2016 | 2016 |
| Modulation Scheme | OFDM | DSSS/ CCK | DSSS/CCK và OFDM | OFDM và DSSS/CCK | OFDM và DSSS/CCK |  |  | OFDM |
| Tốc độ dữ liệu | 6,9,12, 18,24, 36,48, 54 Mbps | 1,2,5.5and 11Mbps | 54Mbps | 72Mbps |  | 200 Mbps, 400 Mbps, 866Mbps, 1.73Gbps | 200Mbps, 400Mbps, 433Mbps, 600Mbps, 867Mbps | 8 Gbps |
| Sóng mang RF | 5GHz | 2.4Ghz | 2.4GHz | 2.4 GHz và 5.0 GHz | 5 GHz |  |  | 60 GHz |
| Tốc độ lý thuyết | 54 Mbps | 11Mbps | 54 Mbps | 600 Mbps | 1300 Mbps |  |  | 7200Mbps |
| Băng thông | 20MHz |  | 20 MHz | 20MHz và 40MHz | 20 MHz, 40MHz, 80 MHz, 160 MHz | 20 MHz, 40MHz, 80 MHz và 160 MHz | 20,40,80 MHz,160 MHz | 2.16 GHz |
| Khoảng cách bao phủ trong nhà | 35m | 38m | 38m | 70m | 35m |  |  | 60m |
| Khoảng cách bao phủ ngoài trời | 120m | 140m | 140m | 250m |  |  |  | 100m |

## **Trình bày định nghĩa macro mobility. Trình bày về giao thức Mobile ỊP.**

## **Trình bày định nghĩa micro mobility. Trình bày về giao thức cellular lp và giao thức Fast handoff.**

# Câu 1: So sánh macro mobility và micro mobility

Giống :đều là mạng di động kết nối internet.

Khác:

* Macro mobility(tính di động vĩ mô):
* Đây là tính di động thông qua mạng toàn cầu. Trong khi di chuyển trong một mạng như vậy, có thể giao tiếp mà không phá vỡ quyền truy cập hiện có. IP di động, là giao thức quan tâm đến tính di động vĩ mô.
* xảy ra khi MN di chuyển toàn cầu từ MAP này sang MAP khác nằm cách xa nhau
* Micro mobility(Tính di động vi mô):
* Đây là tính di động của một thiết bị trong một miền quản trị duy nhất của mạng toàn cầu. Đối với mạng di động, đây là mức độ di động thấp nhất. IP di động là giao thức được thiết kế để quan tâm đến tính di động vi mô.
* chuyển giao di động vi mô xảy ra khi MN di chuyển cục bộ giữa các bộ định tuyến truy cập trong một miền MAP.

## **Tìm hiều về thành phần của mạng không dây.**

Antennas

Wireless router

Internet port

Wireless access point

Điểm truy cập không dây

Một điểm truy cập trung tâm về cơ bản là không dây tương đương với một trung tâm LAN. Đó là một hộp nhỏ (có một hoặc nhiều ăng-ten) sử dụng đầu nối để gắn nó vào phần còn lại của mạng LAN có dây của bạn.

Các điểm truy cập nhận và truyền dữ liệu từ và đến tất cả các thiết bị không dây trong khu vực của chúng. Chúng có thể xử lý nhiều kết nối khác nhau giữa các thiết bị khác nhau, tất cả đều nói chuyện với nhau cùng một lúc, nhưng bạn càng có nhiều thiết bị làm việc với một điểm truy cập, chúng sẽ hoạt động càng chậm.

Bạn có thể cần nhiều hơn một điểm truy cập để phủ sóng một tòa nhà, tùy thuộc vào phạm vi của tòa nhà và cấu tạo của bất kỳ bức tường hoặc tầng nào giữa điểm truy cập và card mạng không dây.

Thẻ giao diện mạng không dây (NIC)

Thẻ giao diện mạng đóng vai trò là bộ thu và phát radio cho một máy tính cụ thể và kết nối nó vào mạng WLAN. Nó được kết hợp với hệ điều hành thiết bị bằng trình điều khiển phần mềm. Nhiều máy tính xách tay hoặc máy tính bảng hiện đại có tích hợp khả năng Wi-Fi này, nhưng với các máy tính để bàn cũ hơn, bạn có thể cần phải cài đặt một tính năng.

Hầu hết các card mạng không dây đều kết nối với một điểm truy cập. Tuy nhiên, một số NIC có thể kích hoạt kết nối ngang hàng - tức là chúng có thể nói chuyện với các card mạng tương thích khác nằm trong phạm vi của nó. Điều này có thể hữu ích cho các nhóm làm việc chuyển vùng nhỏ của các thiết bị không yêu cầu quyền truy cập vào đường trục LAN.

Bộ phát wifi

Trung tâm của một mạng không dây là một bộ định tuyến không dây. Thiết bị này cho phép các thiết bị không dây và thậm chí có dây kết nối với internet.

Hầu hết các bộ định tuyến không dây hiện đại đều tích hợp điểm truy cập không dây, bộ định tuyến và bộ chuyển mạch ethernet vào một thiết bị. Điều này cho phép ba chức năng của các thành phần này được cấu hình và quản lý trong bộ định tuyến. Điều này được thực hiện thông qua giao diện quản lý và phần cứng của bộ định tuyến.

Do đó, bộ định tuyến không dây có thể cho phép thiết bị không dây hoặc có dây truy cập internet thông qua modem cáp, DSL hoặc ADSL.

Một số bộ định tuyến không dây nâng cao có cổng song song để cho phép chúng hoạt động như máy chủ in.

Điểm truy cập không dây (WAP) hoặc Điểm truy cập (AP)

Điểm truy cập là một thiết bị chứa thẻ radio giao tiếp với các thiết bị người dùng riêng lẻ trên mạng cục bộ không dây hoặc mạng WLAN. Các điểm truy cập cũng có một NIC có dây giao tiếp với hệ thống phân phối mạng như Ethernet.

Phần mềm hệ thống được cài đặt trong điểm truy cập làm cầu nối giữa mạng WLAN và phía phân phối có dây. Do đó, điểm truy cập cung cấp kết nối không dây đến mạng LAN có dây còn lại, nhận và truyền dữ liệu đến tất cả các thiết bị không dây trong một khu vực cụ thể.

Các điểm truy cập cũng quản lý nhiều kết nối trong mạng không dây. Tuy nhiên, nếu một WAP bị quá tải với nhiều thiết bị, hiệu suất tổng thể của mạng sẽ giảm xuống. Một hoặc nhiều điểm truy cập thường là đủ cho một văn phòng hoặc tòa nhà nhỏ.

Hầu hết các điểm truy cập trông giống như một hộp nhỏ có nhiều ăng-ten, đồng nghĩa với vẻ ngoài của một bộ định tuyến. Và mặc dù các bộ định tuyến hiện đại cũng tích hợp điểm truy cập không dây, một số thiết bị chỉ phục vụ vai trò này.

Bộ điều hợp không dây hoặc NIC

Bộ điều hợp không dây, còn được gọi là thẻ giao diện mạng không dây (NIC), đóng vai trò là bộ thu và phát sóng vô tuyến cho máy tính hoặc thiết bị được kết nối với mạng không dây. Thành phần này được kết hợp với hệ điều hành của máy tính bằng trình điều khiển phần mềm.

Nhiều máy tính và máy tính xách tay hiện đại được tích hợp khả năng Wi-Fi. Bạn có thể phải cài đặt tính năng này bằng cách sử dụng card mạng được kết nối với bo mạch chủ của máy tính hoặc bên ngoài thông qua giao diện USB đối với các máy tính thế hệ cũ.

Các NIC được thiết kế chủ yếu để kết nối với một điểm truy cập. Tuy nhiên, một số NIC cho phép kết nối ngang hàng. Kiểu kết nối này cho phép các máy tính có card mạng tương thích trong phạm vi có thể giao tiếp.

Kết nối ngang hàng hữu ích cho một nhóm làm việc chuyển vùng nhỏ gồm các thiết bị không cần mạng LAN hoặc internet để hoạt động.

Đài không dây

Cầu nối không dây nhằm mục đích cải thiện vùng phủ sóng Wi-Fi của bạn hoặc mở rộng nó. Mục đích chính của chúng là nhận tín hiệu Wi-Fi hiện có, chuyển tiếp yêu cầu và phản hồi qua lại giữa thiết bị của bạn và điểm truy cập chính hoặc bộ định tuyến Wi-Fi.

Cầu không dây đôi khi được gọi là bộ lặp không dây. Chúng có thể tăng gấp đôi phạm vi của mạng WLAN.

Do đó, một cây cầu không dây cung cấp một liên kết ngoài trời, tốc độ cao, tầm xa giữa các tòa nhà. Hầu hết các cây cầu có phạm vi hoạt động khoảng 25 dặm. Chúng thường không bị ảnh hưởng bởi các vùng nước, đường sắt hoặc chướng ngại vật vì chúng dựa trên tầm nhìn.

Tuy nhiên, phạm vi của hầu hết các mạng WLAN thường sẽ bị ảnh hưởng bởi các điểm truy cập trong mạng. Hầu hết các mạng WLAN đều có điểm truy cập với ăng-ten hoặc ăng-ten đa hướng truyền tín hiệu theo mọi hướng.

Mặt khác, một số mạng WLAN sử dụng các điểm truy cập có ăng-ten định hướng tạo ra tín hiệu tập trung hơn bao phủ một khu vực hẹp hơn. Do đó, bạn có thể cần thay thế ăng-ten trên điểm truy cập không dây của mình để có phạm vi phủ sóng tốt hơn.

Bộ điều khiển không dây

Bộ điều khiển không dây là cần thiết khi mạng không dây cần nhiều điểm truy cập không dây. Công việc của bộ điều khiển không dây là cung cấp một nền tảng quản lý Wi-Fi tập trung để quản lý tất cả các điểm truy cập trong mạng.

Với bộ điều khiển không dây, bạn có được các tính năng và khả năng quản lý nâng cao như kiểm soát truy cập, xác thực tập trung và khả năng hạn chế băng thông trên cơ sở nhóm hoặc người dùng. Bạn cũng có thể thực hiện ưu tiên lưu lượng và Chất lượng dịch vụ (QoS)

## **Tìm hiểu hoạt động của mạng không dây.**

❖ Infrastructure Mode

❖ Ad hoc Mode

❖ Tethering

❖ Basic Service Set (BSS)

❖ Extended Service Set (ESS)

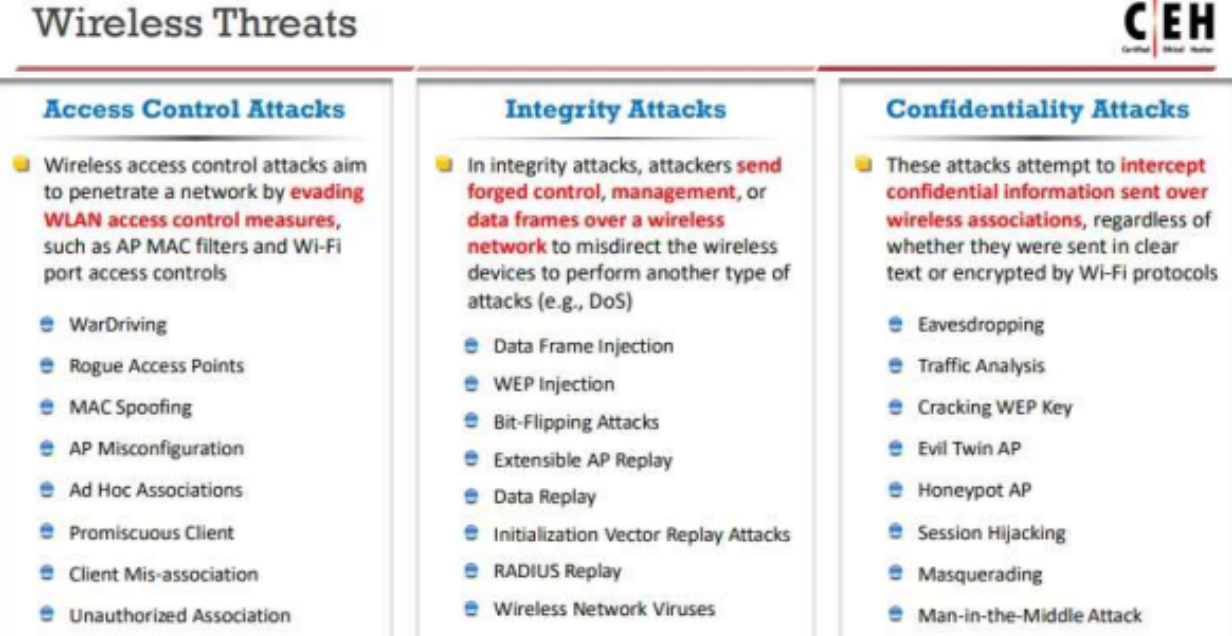
❖ 802.11 Frame Structure

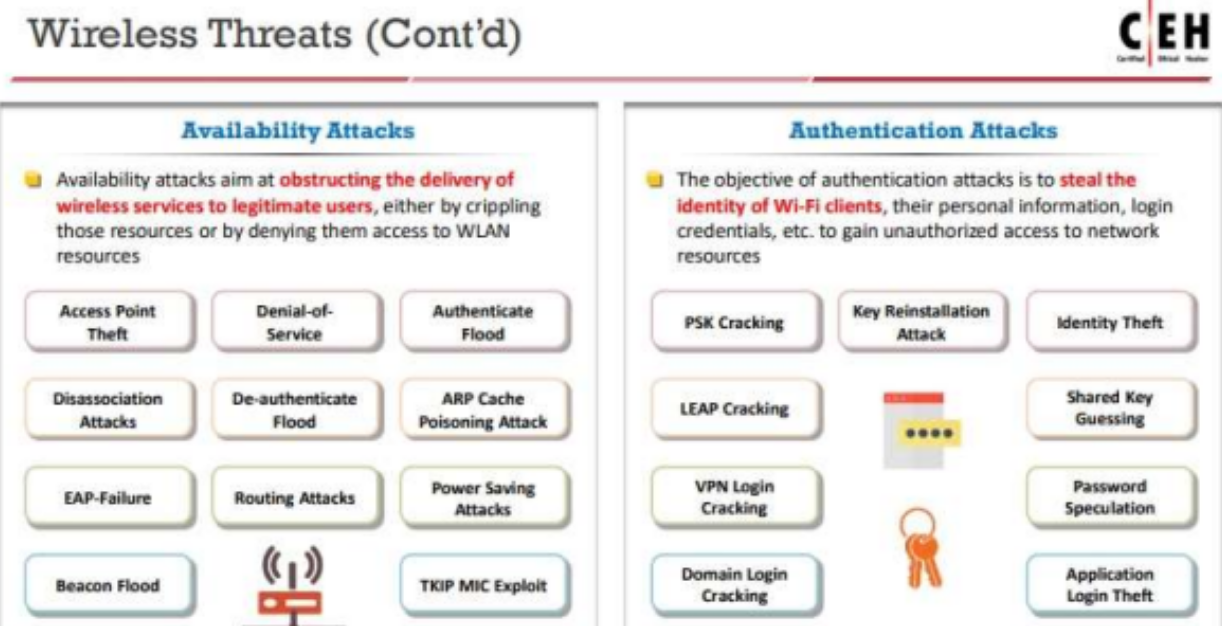
❖ Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)

❖ Wireless Client AP Association

❖ Passive and Active Delivery Mode

## **Tìm hiểu các mối đe doạ và các cuộc tấn công lên mạng không dây.**





Mối đe dọa:

❖Chặn bắt dữ liệu

❖Tấn công xâm nhập mạng không dây

❖Tấn công từ chối dịch vụ

❖Giả mạo AP

Các cuộc tấn công:

Tấn công bị động (nghe trộm – Passive attacks).

❖ Tấn công chủ động (kết nối, dò và cấu hình mạng -Activeattacks).

❖ Tấn công kiểu chèn ép (Jamming attacks).

❖ Tấn công theo kiểu thu hút (Man–in-the-middle attacks).

❖ Tấn công lặp lại (Replay attacks).

## **Tìm hiểu về WEP, WPA, WPA2, WPA3 và so sánh các giao thức trên.**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **WEP** | **WPA** | **WPA2** |
| **Năm phát hành** | 1997 | 2003 | 2004 |
| **Thuật toán mã hóa** | RC4 | TKIP với RC4 | CCMP và AES |
| **Độ dài khóa** | 40 bit | 128 bit | 128 bit |
| **Độ dài Initialization Vector** | 24 bit | 48 bit | 48 bit |
| **Quay vòng khóa** | không | Các khóa phiên động | Các khóa phiên động |
| **Toàn vẹn dữ liệu** | CRC-32 | Mã MIC – sử dụng thuật toán Michael-64 | CCMP (Counter Mode CBC-MAC Protocol) |
| **Toàn vẹn cho phần header** | CRC-32 | Địa chỉ nguồn/đích được bảo vệ bởi thuật toán Michael-64 | CBC-MAC |
| **Quản lý khóa** | Không cung cấp | Cơ chế bắt tay 4 bước | Cơ chế bắt tay 4 bước |
| **Xác thực** | Open system/Shared key | Pre-Shared Key(PSK), 802.1x & EAP | PSK, 802.1x/EAP (TKIP, EAP-TLS) |
| **Phân phối khóa** | Thủ công | 802.1x (EAP) | 802.1x (EAP) |
| **Chống relay attack** | không | có | có |

## **Trình bày các thách thức bảo mật của Apple.**

* Apple từ trước đến nay chậm đưa ra các bản vá cho các lỗ hổng đã biết được sửa trong các

thành phần mã nguồn mở được sử dụng trong OS X.

* Apple cũng vá các lỗi phần mềm của riêng họ trên các lịch trình khác nhau cho các nền tảng

khác nhau, có khả năng khiến người dùng gặp nhiều rủi ro hơn.

* Apple phải đối mặt với một số thách thức bảo mật khác nữa. Việc bẻ khóa dựa trên việc khai

thác các lỗ hổng bảo mật, cho nên khi bản bẻ khóa mới được phát hành, nó có thể cung cấp

cho những kẻ tấn công một cách khác để tấn công thiết bị iOS.

## **Trình bày các giải pháp bảo mật đối với Apple iOS.**

* An toàn phần cứng

Để phần mềm an toàn thì phần mềm đó phải dựa trên phần cứng được tích hợp an toàn:

▪ Secure boot: được thiết kế để bảo vệ phần mềm ở những mức thấp nhất, nó chỉ cho phép phần mềm hđh từ Apple được tải vào phần khởi động

▪ AES engines: đảm bảo việc mã hóa lưu trữ được nhanh chóng và hiệu quả trong khi không làm lộ dữ liệu mà nó sử dựng để thiết lập các mối quan hệ khóa mật mã.

▪ Secure Enclave:

❑ Là một hệ thống trên chip (SoC).

❑ Tuân theo nguyên tắc thiết kế tương tự như SoC, chứa ROM boot và AES engines riêng.

❑ Cung cấp nền tảng cho việc tạo và lưu trữ an toàn các khóa cần thiết để mã hóa dữ liệu ở trạng thái nghỉ, đồng thời bảo vệ và đánh giá dữ liệu sinh trắc học cho Face ID và Touch ID.

* An toàn hệ thống

An toàn hệ thống chịu trách nhiệm kiểm soát quyền truy cập vào tài nguyên hệ thống trong các thiết bị của Apple mà không ảnh hưởng đến khả năng sử dụng.

An toàn hệ thống bao gồm quá trình khởi động, cập nhật phần mềm và bảo vệ tài nguyên hệ thống máy tính như CPU, bộ nhớ, đĩa, chương trình phần mềm và dữ liệu được lưu trữ.

Một phần quan trọng trong bảo mật của Apple là secure boot, bảo vệ hệ thống khỏi bị nhiễm phần mềm độc hại tại thời điểm khởi động. Secure boot bắt đầu từ phần cứng và xây dựng một chuỗi tin cậy thông qua phần mềm, trong đó mỗi bước được thiết kế để đảm bảo rằng bước tiếp theo hoạt động bình thường trước khi chuyển giao quyền kiểm soát.

Hệ thống cập nhật được thiết kế để ngăn chặn các cuộc tấn công hạ cấp để thiết bị không thể quay trở lại phiên bản hệ điều hành cũ hơn (mà kẻ tấn công biết cách xâm nhập) như một phương pháp đánh cắp dữ liệu người dùng.

Các thiết bị của Apple cũng bao gồm các biện pháp bảo vệ khởi động và thời gian chạy để chúng duy trì tính toàn vẹn trong quá trình hoạt động liên tục.

* Mã hóa và bảo vệ dữ liệu

Các thiết bị iOS và iPadOS sử dụng phương pháp mã hóa tệp được gọi là Data protection, trong khi dữ liệu trên máy Mac chạy Intel được bảo vệ bằng công nghệ mã hóa khối lượng được gọi là FileVault.

Hệ thống phân cấp quản lý khóa được bắt nguồn từ silicon chuyên dụng của Secure Enclave, AES Engine chuyên dụng hỗ trợ mã hóa tốc độ đường truyền và giúp đảm bảo rằng các khóa mã hóa lâu dài không bị lộ với nhân hđh hoặc CPU .

Apple sử dụng nhân hệ điều hành để thực thi bảo vệ và bảo mật. Kernel sử dụng điều khiển truy cập cho các ứng dụng hộp cát và một cơ chế được gọi là Data Vault.

* An toàn ứng dụng

▪ Apple cung cấp các lớp bảo vệ để giúp đảm bảo rằng các ứng dụng không có phần mềm độc hại đã biết và không bị giả mạo

▪ Tất cả các ứng dụng đều được tải xuống từ App Store — và tất cả các ứng dụng đều được đưa vào hộp cát — để cung cấp các biện pháp kiểm soát chặt chẽ nhất.

▪ Đối với các ứng dụng không tải từ App Store thì phải được kiểm chứng bởi Apple mới có thể khởi chạy

* An toàn dịch vụ

Apple đã xây dựng một bộ dịch vụ mạnh mẽ để giúp người dùng nhận được nhiều tiện ích và năng suất hơn từ thiết bị của họ. Các dịch vụ này cung cấp các khả năng mạnh mẽ cho lưu trữ đám mây, đồng bộ hóa, lưu trữ mật khẩu, xác thực, thanh toán, nhắn tin, liên lạc và hơn thế nữa, tất cả đồng thời bảo vệ quyền riêng tư của người dùng và bảo mật dữ liệu của họ.

* An toàn mạng

Ngoài các biện pháp bảo vệ tích hợp mà Apple sử dụng để bảo vệ dữ liệu được lưu trữ trên các thiết bị của Apple, có nhiều biện pháp mà các tổ chức có thể thực hiện để giữ an toàn cho thông tin khi nó di chuyển đến và đi từ một thiết bị. Tất cả các biện pháp và biện pháp bảo vệ này đều thuộc phạm vi an ninh mạng:

An toàn TLS

An toàn truyền tải ứng dụng

App Transport Security cung cấp các yêu cầu kết nối mặc định để ứng dụng tuân thủ các phương pháp hay nhất về kết nối an toàn khi sử dụng các API NSURLConnection, CFURL hoặc NSURLSession. Theo mặc định, App Transport Security giới hạn lựa chọn mật mã để chỉ bao gồm các bộ cung cấp bí mật chuyển tiếp, cụ thể:

• ECDHE\_ECDSA\_AES và ECDHE\_RSA\_AES trong Galois / Counter Mode (GCM)

• Chế độ chuỗi khối mật mã (CBC)

▪ Kiểm tra tính hợp lệ của chứng chỉ:

• Các thiết bị của Apple được cập nhật định kỳ với danh sách hiện tại các chứng chỉ bị thu hồi và hạn chế.

• Danh sách được tổng hợp từ các danh sách thu hồi chứng chỉ (CRL), được xuất bản bởi từng tổ chức phát hành chứng chỉ gốc tích hợp được Apple tin cậy, cũng như các tổ chức phát hành CA cấp dưới của họ.

An toàn IPv6

IPv6 được tạo ra khi SLAAC ( Stateless Address Autoconfiguration) được sử dụng

▪ Thuật toán tạo địa chỉ dựa vào chuẩn RFC 3972 nhằm đảm bảo các giao diện khác nhau trong cùng một mạng sẽ có địa chỉ khác nhau

▪ Các địa chỉ tạm thời chỉ tồn tại trong 24 tiếng đối với bất cứ một kết nối mới nào.

▪ Để bảo vệ chống lại các cuộc tấn công dựa trên tiêu đề mở rộng IPv6 và phân mảnh, Các thiết bị của Apple thực hiện các biện pháp bảo vệ được chỉ định trong RFC 6980, RFC 7112 và RFC 8021.

▪ Để giúp đảm bảo độ tin cậy của ngăn xếp IPv6 của hệ điều hành Apple, các thiết bị của Apple thực thi các giới hạn khác nhau đối với cấu trúc dữ liệu liên quan đến IPv6, chẳng hạn như số tiền tố trên mỗi giao diện.

An toàn VPN

Hệ điều hành iOS, iPadOS và macOS hỗ trợ các giao thức và phương thức xác thực sau:

▪ IKEv2: Hỗ trợ cho cả IPv4 và IPv6 và những thứ sau:

• Phương thức xác thực: Bí mật được chia sẻ, chứng chỉ, EAP-TLS và EAP-MSCHAPv2

• Mật mã Suite B: Chứng chỉ ECDSA, mã hóa ESP với GCM và Nhóm ECP cho Nhóm Diffie-Hellman

• Các tính năng bổ sung: MOBIKE, phân mảnh IKE, chuyển hướng máy chủ, chia đường hầm

▪ L2TP qua IPsec: Xác thực người dùng bằng mật khẩu MS-CHAP v2, mã thông báo hai yếu tố, chứng chỉ, xác thực máy bằng khóa bí mật được chia sẻ hoặc chứng chỉ

▪ SSL VPN: Xác thực người dùng bằng mật khẩu, mã thông báo hai yếu tố và chứng chỉ bằng ứng dụng khách VPN của bên thứ ba

▪ Cisco IPsec: Xác thực người dùng bằng mật khẩu, mã thông báo hai yếu tố và xác thực máy bằng chứng chỉ và bí mật được chia sẻ VPN on demand: VPN Theo Yêu cầu cho phép các thiết bị Apple tự động thiết lập kết nối khi cần thiết. Nó yêu cầu một phương thức xác thực không liên quan đến tương tác của người dùng

▪ Per App VPN: các kết nối VPN có thể được thiết lập trên cơ sở từng ứng dụng, điều này cung cấp khả năng kiểm soát chi tiết hơn đối với dữ liệu nào đi qua VPN. Khả năng tách biệt lưu lượng truy cập ở cấp ứng dụng này cho phép tách dữ liệu cá nhân khỏi dữ liệu tổ chức — dẫn đến kết nối mạng an toàn cho các ứng dụng sử dụng nội bộ, đồng thời bảo vệ quyền riêng tư của hoạt động thiết bị cá nhân

▪ Always on VPN: cho phép toàn quyền kiểm soát lưu lượng truy cập iOS và iPadOS bằng cách chuyển tất cả lưu lượng IP trở lại. Giao thức đường hầm mặc định, IKEv2, đảm bảo việc truyền tải lưu lượng bằng mã hóa dữ liệu.

An toàn Wifi

▪ Truy cập an toàn vào mạng không dây

• Tất cả các nền tảng của Apple đều hỗ trợ các giao thức mã hóa và xác thực Wi-Fi, để cung cấp quyền truy cập được xác thực và tính bảo mật khi kết nối với các mạng không dây an toàn vd: WPA2, WPA 3, PMF.

• Hệ điều hành của Apple bảo vệ thiết bị khỏi các lỗ hổng trong phần sụn vi xử lý mạng. Điều này có nghĩa là bộ điều khiển mạng có Wi-Fi có quyền truy cập hạn chế vào bộ nhớ Bộ xử lý ứng dụng

▪ Tính riêng tư của Wifi

• Sử dụng địa chỉ MAC ngẫu nhiên : có thể truy cập internet an toàn hơn, giúp chống bị nghe lén, che đi địa chỉ MAC thật sự của thiết bị và giúp ẩn danh một phần.

• Sử dụng số thứ tự khung ngẫu nhiên: giúp tránh khỏi việc dò quét thông tin

• Sử dụng mạng wi-fi với SSID ẩn.

❑ An toàn Bluetooth

▪ Có hai loại Blue tooth: Bluetooth classic và Blue tooth Low Energy

▪ Mô hình an toàn Bluetooth:

• Pairing

• Bonding

• Authentication

• Ecryption

• Message integrity

• Secure simple pairing.

▪ Đối với Bluetooth Low Energy: Sử dụng phân phối khóa truyền chéo ( Cross-transport key derivation), địa chỉ ngẫu nhiên để đảm bảo thính bảo mật của người dùng

❑ An toàn chia sẻ mật khẩu Wifi

▪ Sử dụng cơ chế xác thực giống như AirDrop

❑ An toàn tường lửa

▪ Chặn tất cả các kết nối đến, bất kể ứng dụng nào.

▪ Tự động cho phép phần mềm cài sẵn nhận các kết nối đến.

▪ Tự động cho phép phần mềm đã tải xuống nhận các kết nối đến.

▪ Thêm hoặc từ chối quyền truy cập dựa trên các ứng dụng do người dùng chỉ định.

▪ Ngăn Mac phản hồi với các yêu cầu thăm dò ICMP và quét cổng.

❑ An toàn Single-sign-on

▪ Được thiết kế để cải thiện trải nghiệm đăng nhập của người dùng vào các ứng dụng và trang web.

▪ Kerberos là một giao thức xác thực phổ biến được sử dụng trong các mạng lớn cho SSO.

▪ Để xác thực người dùng, các thiết bị Apple phải liên hệ với KDC qua kết nối mạng.

▪ MacOS ưu tiên Kerberos cho tất cả các hoạt động xác thực khi được tích hợp vào môi trường Active Directory.

▪ SSO mở rộng: được sử dụng khi ứng dụng web cần định danh nhà cung cấp để xác thực người dùng.

▪ Có hai loại SSO mở rộng:

• Chuyển hướng đến HTTPS

• Sử dụng cơ chế thử thách / phản hồi như Kerberos.

❑ An toàn Air-drop

▪ AirDrop là một tính năng do Apple phát triển, cho phép chuyển nội dung dữ liệu giữa các thiết bị chạy hệ điều hành OS.

▪ AirDrop sử dụng Bluetooth Low Energy (BLE) và Wi-Fi peet-to-peer để chia sẻ tệp giữa các thiết bị Apple.

▪ AirDrop sử dụng các dịch vụ iCloud để giúp người dùng xác thực. An toàn mạng không dây

* Bộ bảo mật dành cho nhà phát triển

Apple cung cấp một số khung “kit” để cho phép các nhà phát triển bên thứ ba mở rộng các dịch vụ của Apple. Các khuôn khổ này được xây dựng với sự riêng tư và bảo mật của người dùng là cốt lõi của chúng:

HomeKit

CloudKit

SiriKit

DriverKit

ReplayKit

ARKit

* Quản lý thiết bị an toàn Các tổ chức có thể sử dụng các tài nguyên như bảo vệ bằng mật khẩu, hồ sơ cấu hình, xóa từ xa và các giải pháp quản lý thiết bị di động (MDM) của bên thứ ba để quản lý nhóm thiết bị và giúp bảo mật dữ liệu của công ty, ngay cả khi nhân viên truy cập dữ liệu này trên thiết bị cá nhân của họ.

Trong iOS 13 trở lên, iPadOS 13.1 trở lên và macOS 10.15 trở lên, thiết bị Apple hỗ trợ tùy chọn đăng ký người dùng mới được thiết kế đặc biệt cho các chương trình BYOD. Việc đăng ký người dùng cung cấp nhiều quyền tự chủ hơn cho người dùng trên thiết bị của riêng họ, đồng thời tăng cường bảo mật cho dữ liệu doanh nghiệp bằng cách lưu trữ dữ liệu đó trên một ổ đĩa APFS (Hệ thống tệp của Apple) riêng biệt, được bảo vệ bằng mật mã. Điều này cung cấp sự cân bằng tốt hơn về bảo mật, quyền riêng tư và trải nghiệm người dùng cho các chương trình BYOD.

## **Trình bày các thách thức bảo mật của Android.**

❑ Phân mảnh

▪ Những thiết bị Android khác nhau đang chạy trên các phiên bản khác nhau của hệ điều hành này.

❑ Mã độc

▪ Ước tính trung bình có khoảng 11,7 nghìn mẫu mã độc Android mới được phát hiện mỗi ngày.

▪ Phần lớn các cuộc tấn công này nhắm vào các dịch vụ ngân hàng trực tuyến và các ứng dụng di động.

▪ Phần mềm độc hại cryptojacking.

❑ Lựa chọn công cụ quản lý

Bộ quản lý di động doanh nghiệp (EMM) có thể giúp cải thiện bảo mật thiết bị Android với các tính năng quản lý nội dung, ứng dụng và danh tính của chúng. Các yếu tố chính cần tìm là hỗ trợ đa nền tảng - đặc biệt là trên nhiều phiên bản Android - và tích hợp với các hệ thống quản lý hoạt động khác. Những khả năng này ngày càng trở nên quan trọng để tránh các tính năng chồng chéo hoặc xung đột, cũng như để tối đa hóa năng suất CNTT.

❑ Hành vi của người sử dụng:

▪ Người sử dụng luôn đóng vai trò quan trọng trong việc bảo đảm an toàn cho thiết bị cũng như dữ liệu chứa trong nó.

▪ Các chính sách an toàn yêu cầu người dùng sử dụng mật khẩu, sao lưu và lưu trữ thích hợp và tuân thủ các phương pháp tốt nhất để tránh các cuộc tấn công kỹ thuật xã hội.

▪ Người sử dụng có nhiều tầng lớp: Lớp thanh niên, người già, trẻ nhỏ. Mỗi một tầng lớp có sự am hiểu về kỹ thuật và tần xuất và nhu cầu sử dụng khác nhau.

❑ Sự phân chia (Compartmentalization)

▪ Các thiết bị Android hỗ trợ các công nghệ cho phép tách môi trường làm việc và môi trường cá nhân nhưng vẫn đảm bảo các tiêu chí an toàn.

▪ Android 7.0 Nougat có nhiều tính năng hỗ trợ việc phân tách dữ liệu cá nhân và dữ liệu của công ty.

## **Trình bày giải pháp đảm bảo an toàn của Android.**

## **Trình bày về BYOD.**

* BYOD là gì

▪ BYOD (Bring your own device) – “mang theo thiết bị của riêng mình”

▪ Các công ty cho phép nhân viên sử dụng thiết bị của riêng họ ở nhà, tại văn phòng hoặc bất kỳ vị trí nào khác để công việc trở nên dễ dàng hơn

* Xu hướng sử dụng BYOD
* Những lợi ích khi áp dụng byod

▪ Tiết kiệm chi phí

▪ Không cần đến training

▪ Chủ động cập nhật công việc liên tục

▪ Tăng hiệu quả, hiệu suất

▪ Sự hài long của nhân viên

* Thách thức

▪ Dễ mất tập trung

▪ Thiếu nhất quán

▪ Bảo mật lỏng lẻo

▪ Rắc rối khi thu thập dữ liệu (Data retrieval)

* Rủi ro về an toàn

▪ Lây nhiễm mã độc

▪ Thiết bị bị mất hoặc đánh cắp

▪ Việc truy cập mạng không an toàn

* Chính sách bảo mật

Bảo mật BYOD cần quan tâm đến hai điều:

▪ Bảo vệ tài nguyên của công ty (mạng, dữ liệu công ty, ứng dụng, v.v.) khỏi bất kỳ rủi ro an ninh mạng nào bắt nguồn từ thiết bị BYOD được nhân viên sử dụng.

▪ Bảo mật của BYOD phải ngăn chặn việc lây nhiễm phần mềm độc hại, chiến dịch lừa đảo và các mối đe dọa bảo mật khác có thể làm tổn hại đến dữ liệu nhạy cảm và lây lan theo chiều ngang.

Các yếu tố cần được xem xét trong chính sách bảo mật của BYOD:

▪ Các thiết bị và hệ điều hành (OS) cụ thể, bao gồm cả các phiên bản OS, mà một công ty hỗ trợ để sử dụng liên quan đến công việc.

▪ Các ứng dụng và trang web chính có trong danh sách chặn và danh sách cho phép của công ty.Cách thức truy cập an toàn vào đám mây, SaaS, web và các ứng dụng tại chỗ thông qua phần cứng BYOD.

▪ Cách các điểm cuối BYOD sẽ được đăng ký, định cấu hình và hỗ trợ bởi CNTT.

▪ Quyền sở hữu và quản lý dữ liệu thiết bị

▪ Yêu cầu về độ mạnh của mật khẩu

▪ Bất kỳ biện pháp bảo mật nào khác, chẳng hạn như triển khai xác thực đa yếu tố (MFA) và đăng nhập một lần (SSO), mà người dùng BYOD sẽ phải tuân theo.

▪ Cách thức và thời điểm các cấp độ truy cập sẽ thay đổi để đáp ứng với các trạng thái bảo mật của thiết bị.