Case study

1 - بيحصل عمليه mac address filtering في ال NIC بيتحقق من ال Destination mac address in the frame لو مش بيطابق عنوان ال mac الخاص بال NIC بيتم تجاهل ال frame.

---

2 - في ال. Hub كل الاجهزه متوصله علي نفس ال medium لو في جهازين بعتوا في نفس الوقت بيحصل collision domain وال data بتوقع وبيتعملها retransmit تاني ف بيحصل بطئ في الشبكه ، هنا بقي بييجي دور ال switchوبتحل المشكله بانها تعمل separate collision domain for each port واستخدام ال full-duplex communication مما يسمح للاجهزه بالارسال والاستقبال في نفس الوقت بدون حدوث أي collisions .

---

3 - ال FCS(Frame Check Sequence) بيتكون من بايت٤

الهدف منو يكشف الأخطاء في ال. CRC in Ethernet frames وبيدور علي ال البيانات التالفه ولا مش بيصحح أي خطا ولا بيضمن وصوله .

---

4 - ال 48 bytes and 1520 bytes دول خارج نطاق الرينج اللي مسموح بيهم يعدوا علي ال switch

المفروض الرينج بين ال Valid Ethernet size: 64 →1518
أي frame اصغر او اكبر من ال size دا ال. Switch بيسقطهم ومبيعديش ال data.

---

5 - اول ما ال switch يشتغل بيكون mac table فاضي اللي بيحصل ان ال switch بيستقبل ال frame من port pc-A ويسجل ال MAC بتاع ال. PC-A مع ال port فيmac-table بعد كدا بيدور علي ال mac بتاع ال. PC-D في ال mac table مش بيلاقيه فيرجع يبعت ال farme لكل ال ports ماعدا PC-A اول مره بيفصل floodingبعد كدا. ال switch بيعرفع مكان الاجهزه ويبدا يوجه ال الترافيك بدقه.

---

6 - يفضل استخدام تقنيه store-and-forword في ال VoIP علشان بتتحقق من ال frame كامل ولا لا قبل اعاده توجيهه علشان تتمضن انو وصل بدون أي error وجوده خدمه افضل QoS وبالتالي بتزود ال reliability مقارنه بال Cut-through اللي بتبعت ال frames بدون التحقق الكامل.

---

7 - ال ip مبيعملش أي session mode بدون اتصال ولا بيضمن تسليم البيانات او ترتيبها علي عكس ال TCP هو اللي بيضمن وصول البيانات بشكل صحيح ومنظم وبيستدعي أي داتا وقعت .

8 - ال pc يقدر يوصل للطابعه والاجهزه داخل نفس الشبكه علشان هما في نفس ال subnet الاتصال بيتم مباشر في ال layer2 من غير ما نحتاج Router ، بينما ال pc ميقدرش يوصل لاي جهاز خارج الشبكه لا الترافيك علشان تتبعت لشبكات تانيه بتحتاج Default Gateway اللي هو ال Router من غيرو ميعرفش ال pc يوجه الباكت خارج الشبكه المحليه علشان كدا الترافيك بيوقع .
علشان نحل المشكله دي لازم تكوين ال Default Gateway علي ال pc باستخدام ال ip الخاص بالروتر علشان يقدر يخرج لاي شبكه خارجية.

---

9 - ال ARP protocol بيستخدم ال Broadcasts علشان هو ميعرفش عنوان ال mac فبيبعت لكل الاجهزه ويعمل Congestion في الترافيك وبيزود ال load وبطئ الشبكه ، الخطر الأمني ان يمكن استغلاله من خلال ال ARP spoofing وانتحال أي جهاز علي الشبكه ويعرف ب(man-in-the-middle)

---

10 - في ال ipv6 مفيش ARP في حاجه بديله هي ال NDP (Neighbor Discovery Protoclo) ودا بيشتغل باستخدام ال ICMPv6 ، الجهاز بيعت يسآل عن ال ip والجهاز بيرد علي بال mac-address .

---

1 1 - في Hub Ethernet بتشارك في نفس الوسط + ان الاجهزه بتبعت في نفس الوقت فبيحصل collisionويضطروا يعملوا اعاده ارسال (CSMA/CD) وده بيسبب بطئ ، علي عكس ال WI-FI بيتم استخدام (SCMA/CA) فالاجهزة بتنتظر دورها وتحاول تتجنب أي تصادم قبل الارسال ،علشان كدا مبيحصلش أي collisions مباشرة لاكن بيحصل delay/latency اعلي .

---

1 2 - الراوتر بيفك ال Ethernet frameوياخذ ال IP packet ثم يعسد تغليفه في ال. PPP frame عند الارسال علي ال WAN يعني ال layer 2 بيختلف من شبكه للتانيه .
ال LLC مش بيتغير وظيفيا لانه بيحدد البروتوكول الاعلي IPv4/IPv6، لكن في ال ppp بيستخدم protocol field بدل ال LLCالتقليدي .

---

1 3 - حصل .loop فبدات الإطارات تلف في الشبكه بشكل مستمر بدون توقف ، ف broadcast frames اتكررت بشكل كبير فحصل Broadcast Storm، ال switch كان كل مره يشوف نفس ال mac جاي من منافذ نختلفه ، فحصل Flappingوتديث مستمر لل MAC table .

---

14 - بيحصل Duplex mismatch لما السيرفر يكون Half-duplex والسويتش full-duplex ، فالسيرفر يشوف ال collisionsاثناء الارسال ، بينما السويتش مبيشوفهاش دا بقي بيسبب retransmissions.

---

15 - في ال IPv4 الراوتر ممكن يعمل fragmentations لو الباكيت اكبر من ال MTU اثناء الطريق ، علي عكس في ال IPv6 الراوترات مش بتقوم بآي fragmentation ولو الباكيت اكبر من ال MTU بيتم اسقاطها ، الحل في ال IPv6 هو ال path MTU Discovery، حيث يقوم المرسل باكتشاف اقل MTUفي المسار ويرسل البيانات بالحجم المناسب من البدايه.

---

16 - الراوتر R3 10.1.1.0/24 علشان Longest Prefix match واكثر تطابق مع ال ip لو مفيش أي route مطابق يتم استخدام default route ان وجد غير كدا بيحصل drop للباكيت.

---

17 - ال static route ثابت ومش بيكتشف فشل اللينك موجود ولا لا حتي لو المسار وقع, علي عكس ال Dynamic routing بيكتشف الفشل تلقائيا ويحول الترافيك لمسار بديل ويسمي بال (backup path) .

18 - ال ARP مش بيرد علشان ال 10.0.0.50 في شبكه مختلفه ،وال ARPبيشتغل داخل نفس ال subnet فال PC-A مش بيسآل عن السيرفر ، لكنه بيعمل ARPعلي ال Default Gateway علشان ياخد ال mac address بتاعه ويبعتله الترافيك.

19 - في ARP، ال IPv4 بيستخدم broadcastفكل الاجهزه تستقبل الرساله ودا بيعمل ضغط علي الشبكه وال CPU ، علي عكس ال NDP IPv6 بيستخدم Solicited-Node-Multicast فبيبعت لعدد قليل من الاجهزه بدل الكل دا بيزود الكفاءة وبيقلل الحمل علي ال CPU.

20 - PC-A →Router :

IP: 192.168.1.10 → 192.168.2.20

MAC: AA:AA → CC:CC

Router→ Server-B.

IP: 192.168.1.10 → 192.168.2.20

MAC: DD:DD → BB:BB