أسئلة عامة في المقابلات في مجال الدعم الفني (النظام والشبكات)

متى نقول عن جهاز كمبيوتر أنه Domain ومتى نقول Domain controller؟

أي جهاز كومبيوتر يحتوي على (windows server) يسمى domain ولكن عند تفعيل الـ active directory عليه يسمى domain controller.

ماذا تعرف عن الـ AD؟

AD اختصار لـ Active Directory وهو عبارة عن قاعدة بيانات لكل موارد الشبكة والخدمات والمستخدمين بحيث يمكن من خلاله عمل تحكم مركزي بكل هذه الأجزاء في الشبكة والتحكم بصلاحيات المصادقة والتفويض (authentication and authorization).

ما هو الـ Domain؟

هو عنوان الموقع الذي تكتبه في المتصفح للوصول إليه وهو يحل محل الـ ip الخاص بالموقع ويستخدم لتسهيل الوصول إلى الموقع المطلوب بسبب صعوبة حفظ الـ ip لأي موقع ويسمى DNS.

ما هي فكرة الـ Database؟

مستند تجتمع فيه البيانات بانتظام وهذا المستند أو القاعدة يصبح ملجأً سهلاً للمطور أو الشركة كي تسحب منه البيانات المحددة التي تريدها وتنظمها حسب ما تريد. تتميز بأنه يمكن جمع عدد كبير منها في مكان واحد ويمكن لمصمم قاعدة البيانات أن يخزن المزيد منها متى ما أراد وإدارتها جميعاً وأيضاً استعادة ما يريد منها وذلك باستخدام نظام إدارة لقاعدة البيانات يعرف اختصاراً بنظم قاعدة البيانات المعاصرة DBMS (Data Base Management System).

SQL (Structured Query Language) هي لغة برمجة تستخدمها تقريباً كل قواعد البيانات الارتباطية للاستعلام عن البيانات ومعالجتها وتعريفها وتسهيل التحكم في الوصول لها.

ماذا تعرف عن POE؟

POE اختصار لـ Power Over Ethernet هي تكنولوجيا حديثة لنقل الطاقة عبر الإنترنت حيث تسمح لكابلات الشبكة لنقل الكهرباء أيضاً من أجل الأجهزة المتصلة بها. تعتمد هذه التقنية على توصيل الإنترنت والكهرباء في وقت واحد للجهاز عن طريق

كابل POE الذي يتكون من أسلاك كهربائية بقدرة ٢٥ واط وأسلاك اتصال شبكي مدمجة في سلك واحد.

ما الفرق بين ram and rom والمسميات لهم من دون اختصار؟

RAM: Random Access Memory

تقوم هذه الذاكرة بحفظ البيانات والمعلومات التي يقوم بها المستخدم وتقوم بتخزينها بشكل مؤقت وعند انقطاع التيار تختفي إذا لم يتم حفظها وهي أسرع من الـ ROM.

ROM: Read Only Memory

تقوم هذه الذاكرة بتخزين برامج التشغيل والبرامج الأساسية التي تقوم بتشغيل جهاز الكمبيوتر ولا يمكن التعديل عليها أو محوها لأنها مخزنة من الشركة المصنعة الرئيسية ولا يمكن لجهاز الكمبيوتر أن يعمل بدونها كما أنّها لا تتأثر بانقطاع التيار الكهربائي عن الجِهاز بل يمكن استعادة بياناتها عند تشغيل الجهاز مرة أخرى.

ما هو الـ encryption؟

التشفير هو تحويل البيانات من شكل قابل للقراءة إلى شكل لا يمكن قراءته أو معالجته إلا بعد فك تشفيره وهو وحدة البناء الأساسية في أمن البيانات وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض سلبية ويستخدم بشكل كبير على الإنترنت لضمان أمان معلومات المستخدم التي ترسل بين المستعرض والخادم.

ما هو الـ fire wall؟

الـ fire wall جهاز يكون بين الـ router والـ switch يقوم بعزل الـ LAN عن الـ WAN لحماية الشبكة من أي جهاز خارجي يريد الدخول.

ما هو الفرق بين الـ proxy والـ firewall؟

الـ proxy والـ firewall متشابهان نوعاً ما ولكنهما يؤديان المهام بطريقة مختلفة. يقوم الـ proxy بمراقبة الاتصال الذي يخرج من الشبكة الداخلية إلى الإنترنت وذلك إما لمنعه أو لإعادة توجهيه وإعطاء صلاحيات معينة له أي أنه من داخل الشبكة إلى خارجها.

أما الـ firewall فيقوم بمراقبة وفحص الاتصالات التي تأتي من خارج الشبكة إلى داخلها لذلك يعتبر هو خط الدفاع الأمامي للشبكة.

الـ proxy تقوم بإخفاء الشبكة الداخلية الخاصة بك من الإنترنت ولكن ال firewall لا يمكنه ذلك.

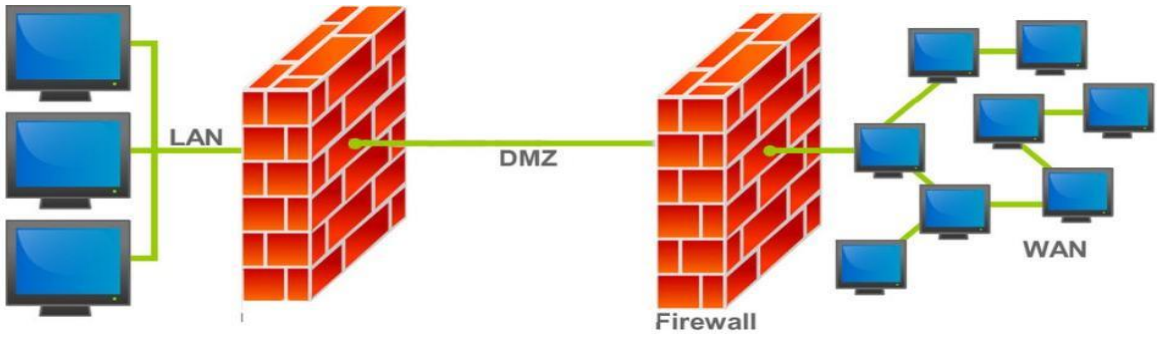
الـ firewall يمكنه إيقاف تشغيل البرامج بينما لا يمكن لـ proxy Server عمل ذلك.
الـ firewall يمكنه حجب الاتصال بينما ال proxy Server يقوم بإعادة توجيه الاتصال لفتح اتصالات محجوبة لديك.

الـ fire wall يعمل في بيانات طبقة الـ network والـ transport. والـ proxy يعمل على بيانات طبقة الـ application.

ماهي وظيفة الـ DMZ؟

DMZ هو اختصار لكلمة Demilitarized Zone والتي يتم ترجمتها إلى منطقة منزوعة السلاح وهو باختصار نوع ثالث من شبكات الإنترنت يقع في مستوى وسط بين الشبكات الداخلية والخارجية.

الصورة أدناه توضح بشكل أكثر تعريف DMZ وكيف يعمل على حماية الشبكة الداخلية.



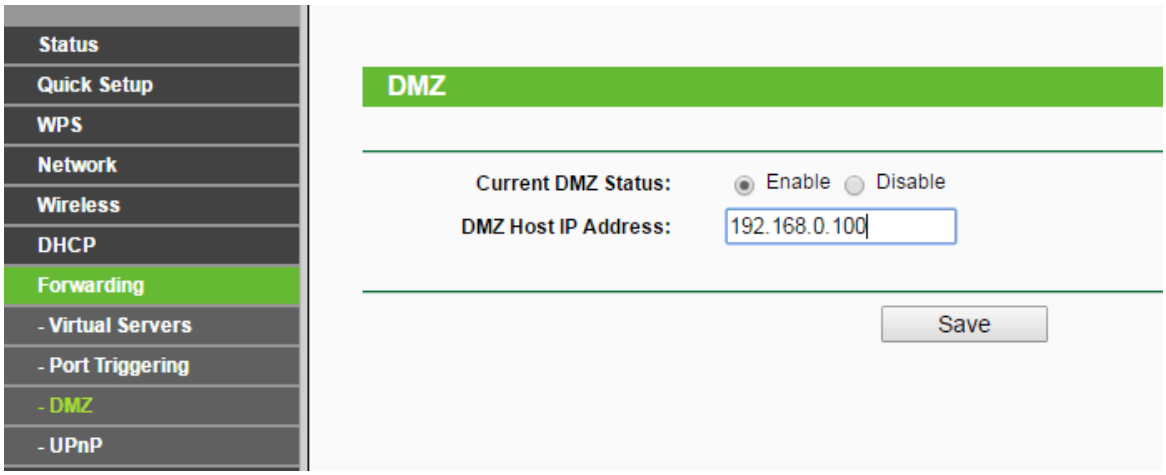
في حالة إذا تم اختراق خدمة في DMZ فإن المهاجم أو المخترق ليس لديه سوى الحصول على معلومات في المنطقة نفسها التي تم الوصول إليها وليس له إمكانية الوصول إلى حواسيب أخرى في الشبكة الداخلية LAN وهي من أفضل المميزات في DMZ.

يتم تفعيل DMZ في شبكة فرعية محددة من أجل حماية بقية الشبكات لأن المخترق إذا نجح في مهاجمة شبكة لن يستطيع الوصول إلى أخرى.

الخدمات في DMZ:

جميع الخدمات التي يتم توفيرها للمستخدمين في شبكة الإنترنت الخارجية يمكن وضعها على dmz مثل FTP وWeb Server وVoIP.

يتوفر dmz في معظم أجهزة الـ router يمكنك البحث عنه في إعدادات الـ router الخاص بك إذا كنت ترغب في تفعيله وحماية الشبكة الخاصة بك، ويتوفر أيضًا في جهاز Access Point كما في الصورة أدناه.



اذكر عدد من بروتوكولات التوجيه؟

.EIGRP, RIP and OSPF

الـ switch والـ hub في أي طبقة؟ والـ router في أي طبقة؟

الـ switch والـ hub في الطبقة الثانية والـ router في الطبقة الثالثة.

هل يوجد switches تعمل في الطبقة الثالثة؟

نعم ويمكن معرفتها من أول رقم في الرقم الخاص بنوع الجهاز.

ما الفرق بين أنواع التشفير Symmetric and Asymmetric؟

Symmetric تعني متماثل أو متناظر ويمكن توضيحها كالتالي:

إذا كنت تريد إرسال رسالة إلى صديقك يتم تمرير هذه الرسالة من خلال خوارزمية التشفير ويتم استخدام المفتاح للتشفير. خوارزمية التشفير هذه متاحة ومعروفة للجميع وقد يأتي شخص ما يريد أن يعرف ما محتوى هذه الرسالة، مفتاح التشفير هو سر بينك وبين صديقك. إذا كان الشخص الذي يريد معرفة محتوى الرسالة hacker وتمكن من اعتراض هذه الرسالة المشفرة، لن يكون قادر على مشاهدتها إلا إذا كان لديه مفتاح فك التشفير. وهذا ما يسمى بالتشفير المتناظر، حيث يتم استخدام نفس المفتاح لتشفير وفك التشفير على كلا الجانبين.

وبما أن الطرفين لهما الحق في الحصول على المفتاح فربما يتم تسريب هذا المفتاح من أحدهما وبالتالي يتم تعريض الرسالة للخطر إذاً فهي ليست فعالة في جميع الحالات ولكن هذا النوع أسرع من التشفير الغير متماثل.

Asymmetric تعني غير متماثل أو غير متناظر ويمكن توضيحها كالتالي:

يتم استخدام نوعين من المفاتيح لكل طرف، المفتاح العام والمفتاح الخاص، كل طرف لديه المفتاح العام وهو معروف لدى الجميع والمفتاح الخاص هو خاص بالمستقبل ولا يعلمه أحد آخر. إذاً المفاتيح العامة متاحة لكل من الطرفين ومتاحة إلى أي شخص آخر حيث يمكن تبادل المفاتيح العامة بالهاتف أو بأي وسيلة اتصال اخرى دون الخوف من أن يتم التنصت عليها لأنها لن تفيد بشيء وحدها.

ما هو بروتوكول HTTP؟ وما الفرق بينه وبين HTTPS؟

HTTP: اختصار لـ Hyper Text Transfer Protocol وهو بروتوكول التواصل حيث يمرر المعلومات بين العميل (الحاسوب الشخصي) وبين الخوادم. HTTPS: اختصار لـ Hyper Text Transfer Protocol Secure ويتم استخدامه للاتصال الآمن عبر الشبكة، ويستخدم على نطاق واسع في شبكة الإنترنت ويعمل على حماية خصوصية وسلامة البيانات المتبادلة أثناء النقل على الشبكة.

البروتوكول	HTTP	HTTPS
العنوان	http://	https://
الأمان	غير آمن	آمن
المنفذ	يستخدم المنفذ 80	يستخدم المنفذ 443
العمل	يعمل في طبقة التطبيق	يعمل في طبقة النقل
شهادات SSL	لا توجد شهادات SSL مطلوبة	يلزم وجود شهادة SSL وموقعة من قبل CA
التحقق من صحة المجال	لا يتطلب التحقق من صحة المجال	يتطلب التحقق من صحة المجال وبعض الشهادات تتطلب التحقق من صحة المستندات القانونية
التشفير	لا يوجد تشفير	يتم تشفير البيانات قبل الإرسال
وقت المعالجة	لا يتطلب أي وقت في المعالجة	يتطلب وقت كثير أثناء المعالجة

ما هو الـ DNS وما فائدته وكيف يمكن تفعيله؟

هو اختصار لـ Domain Name System ويعمل على ترجمة أسماء النطاقات إلى عناوين فمثلاً عند كتابة www.google.com يقوم الـ DNS بإرجاع اسم النطاق وهو74.125.224.72

إذاً فائدته تسهيل الوصول إلى المواقع بكتابة اسمها بدلاً من كتابة عنوانها (الـ IP الخاص بها) حيث تكون العملية أصعب للتذكر.

يمكن الدخول إلى خيارات الـ DNS عن طريق لوحة التحكم ثم مركز الشبكة والمشاركة وبعدها نختار الشبكة المتصل عليها الجهاز وندخل إلى إعداداتها ثم نختار IPv4 فتظهر لنا الإعدادات الخاصة بالشبكة ومن ضمنها الـ DNS حيث يمكن تحديده أوتوماتيكياً أو يدوياً.

ما هو الـ DHCP وما فائدته وكيف يمكن تفعيله؟

هو اختصار لـ Dynamic Host Configuration Protocol.

فائدته: يعمل على توزيع الـ IP للعديد من الأجهزة بشكل أوتوماتيكي.

يمكن تفعيله عن طريق الذهاب إلى server manager ثم اختيار manage في القوائم الرأسية على الزاوية اليمنى وبعدها نختار add rules and features ثم نتبع الخطوات إلى أن نصل إلى الخيار الذي نريده.

ماهي OSI Layers؟

قامت منظمة الـ ISO بعمل نظام موحد لكي يستخدم على مختلف أنظمة التشغيل المختلفة (ويندوز – لينكس – يونكس وغيرها) وذلك لكي يسهل على أنظمة التشغيل أن تتخاطب معاً بلغة موحدة وهذا النظام هو OSI Layers فهو يمثل سبع مراحل تمر من خلالها البيانات من جهاز المرسل مروراً بالشبكة حتى تصل إلى الجهاز المستقبل. مراحل ال OSI السبعة: الترتيب من سبعة إلى واحد على حسب الجهاز المستقبل وليس المرسل.

7- Application:

تمثل فعليا التطبيق الذي نستخدمه.

البروتوكولات المستخدمة:

HTTP, FTP, TFTP, SMTP, SNMP, DNS & Telnet.

6- Presentation:

تمثل اللحظة الفعلية عند إرسال صورة أو ملف أو محادثة لشخص ما (أي تأخذ التعليمات من الطبقة التي قبلها طبقة التطبيقات وتجهزها وتضغطها لكي توفر الحجم وتشفرها لتكون آمنة ولا تختلط بأي بيانات أخرى).

البروتوكولات المستخدمة:

.JPEG, BMP, TIFF, MPEG, WMV, AVI / ASCII & EBCDIC

:Session -5

تأخذ من الطبقة التي قبلها نوع البيانات المطلوب إرسالها للطرف الآخر مغلفة ومضغوطة ومشفرة. أي ستقوم بفتح منفذ يمكن من خلاله للجهاز المرسل والمستقبل التواصل فيما بينهما. ويوجد ثلاثة أنواع من الاتصال:

الأول: يسمى single وهو الاتصال الذي يكون من طرف واحد أي أتلقى معلومات ولا أقدر على الرد عليها مثل التلفاز أسمع منه المعلومات ولكن لا يمكنني التفاعل معه.

الثاني: يسمى half duplex وهو اتصال بين طرفين ولكنه غير متزامن مثل التواصل بين أجهزة اللاسلكي الخاصة برجال الأمن أي لا يمكن الإرسال والاستقبال في نفس اللحظة.

الثالث: يسمى full duplex وهو اتصال بين طرفين ولكنه متزامن مثل مكالمة بين شخصين سواء فيديو أو صوت.

البروتوكولات المستخدمة:

.NFS, NETBIOS NAME, SQL & RPC

:Transport -4

هي الطبقة المسؤولة عن نقل البيانات من مكان إلى مكان آخر وللتوضيح أكثر يمكن تشبيهها بإدارة المرور فهي التي تحدد المسارات والطرقات وهكذا وتسمى البيانات في عند وصولها إلى هذه الطبقة segment.

ويوجد بروتوكولان أساسيان مسؤولان عن عملية نقل البيانات هما:

TCP: Transmission Control Protocol

ينقل البيانات للطرف الآخر وبشكل موثوق ولكنه بطيء. مثل إرسال بريد إلكتروني.

UDP: User Datagram Protocol

ينقل البيانات للطرف الآخر بشكل سريع لكنه غير موثوق. مثل إرسال البيانات في الراديو أو التلفاز أو كاميرات المراقبة.

البروتوكولات المستخدمة: TCP & UDP.

3- Network:

هي التي تحدد أو ترسم الطريق الخاص بمرور البيانات عن طريق الـ router وهو جهاز يحتوي عدة بروتوكولات مسؤولة عن تحديد مسار البيانات بشكل واضح وتقسم إلى ثلاثة أنواع:

الأول: OSBF يبحث عن الطريق الأسرع بغض النظر عن وجود عقبات أو محطات توقف فمثلاً عند وجود مسارين أحدهما بسرعة ٤ ميغا والآخر بسرعة ٢ ميغا فيختار ٤ ميغا.

الثاني: RIP يختار الطريق الأسرع من حيث العقبات ومحطات التوقف وغيرها ويختار الطريق الغير مزدحم بغض النظر عن سرعة نقل البيانات.

الثالث: EIGRP يقوم بعمل عملية حسابية معينة للوصول إلى الهدف بأسرع وقت ممكن بغض النظر عن الطريق سواء بوجود محطات أو عقبات وغيرها.

نعبر عن البيانات في هذه الطبقة بأنها segment + عنوان تم إضافته عن طريق network layer وتسمى بالنهاية Packet.

البروتوكولات المستخدمة: IP & IPX.

2- Data Link:

هنا يتم إضافة عنوان آخر للبيانات لتوضيحها ومعرفة الوجهة التي ستصل إليها ويسمى Mac Address وتسمى البيانات في هذه الحالة frame وهنا تقوم الطبقة بعمل تحديد الخطأ error detection.

البروتوكولات المستخدمة:

Lan protocol:

802.2(llc) – 802.3 (Ethernet)- 802.5 (token ring)- 802.11 (wireless)

Wan protocol:

PPP – frame relay – ATM – ISDN – HDLC

1- Physical:

تمثل عن طريق كرت الشبكة وهنا يتم تحويل إشارة البيانات إلى كهربائية حتى تتمكن من العبور في الوسط الناقل.

الوسائط المستخدمة: Fiber – COAX – ARP.

ما الفرق بين الـ TCP والـ UDP؟

TCP: Transmission Control Protocol

ينقل البيانات للطرف الآخر وبشكل موثوق ولكنه بطيء. مثل إرسال بريد إلكتروني.

UDP: User Datagram Protocol

ينقل البيانات للطرف الآخر بشكل سريع لكنه غير موثوق. مثل إرسال البيانات في الراديو أو التلفاز أو كاميرات المراقبة.

ما هو الـ IP Address والـ MAC Address؟

الـ IP address هو العنوان الذي يأخذه الحاسب للاتصال بالشبكة أو الإنترنت وهو قابل للتغيير ويستخدم من قبل الـ router.

الـ mac address هو العنوان الفيزيائي لكرت الشبكة ويكون وحيد لا يتشابه مع آخر وهو غير قابل للتغيير ويستخدم من قبل الـ switch.

ما هي الـ Vlan؟

هي اختصار لـ Virtual Local Area Network وتعني الشبكة المحلية الوهمية وسميت بذلك لأنه في الواقع عندما تنظر إلى بنيتها تظهر وكأنها شبكة واحدة ولكن في الحقيقة تكون أكثر من شبكة.

تعمل في الطبقة الثانية Data Link Layer والطبقة الثالثة Network Layer.

حيث أن الـ Switch يقوم بتقسيم الشبكة الواحدة إلى عدة شبكات كل منها منفصلة عن الأخرى أي لا يمكن لأجهزة (شبكة افتراضية) الاتصال بأجهزة شبكة افتراضية أخرى مع أنهم مرتبطين بـ Switch وتستخدم لتنظيم الشبكات.

ما الفرق بين الـ router والـ switch وهل الـ switch يعمل في Layer 3؟

Switch	Router
يعمل في الطبقة الثانية	يعمل في الطبقة الثالثة
يتعامل مع الـ mac address	يتعامل مع الـ ip address
يستخدم الـ frames	يستخدم الـ packets
يستخدم في شبكات الـ LAN	يستخدم في شبكات الـ WAN

يوجد طبعاً switches تعمل في الطبقة الثالثة.

ما هو بروتوكول الـ STP؟

STP هو اختصار لـ Spanning Tree Protocol

هو بروتوكول يعمل على تجنب حصول الـ loop بين الـ switches عن طريق إرسال ما يسمى Bridge Protocol Data Unit (BPDU) ومدته من ٢ – ٢٠ ثانية.

ويستخدم في الشبكات المحلية (LAN) ولا يمتد عمله خارجها ويعتبر من بروتوكولات الطبقة الثانية من طبقات الـ TCP/IP والتي تسمى بالـ (Data Link Layer).

عرف الـ port security؟

هي عملية حماية الأجهزة المتصلة على المنافذ عن طريق ربط (توثيق أو تخصيص) الـ mac address للجهاز الذي سيتم توصيله بالمنفذ.

ما المقصود بـ apipa وطرق حل المشكلة؟

APIPA: اختصار لـ Automatic Private IP Addressing ومعناها أن الحاسب يقوم بأخذ IP بشكل اعتباطي في حال عدم الحصول على IP بشكل واقعي ويتم حل المشكلة بإعطاء الحاسب IP بشكل يدوي أو أوتوماتيكي أو alternative.

ما هو الأمر الذي يظهر الـ ip في الشبكة؟

نذهب إلى لوحة cmd ونكتب الأمر: ipconfig/all

حيث يعرض الـ ip address والـ mac address للحاسب.

ما هي عملية الـ ping؟

هي عملية تواصل بين جهازين للتأكد من أن الاتصال بينهما مستقر وناجح ويتم تنفيذه عبر كتابة الأمر: ping x.x.x.x حيث تمثل الـ x العنوان المطلوب الاتصال به (IP) ويتم كتابة الأمر في لوحة cmd أو مباشرة في مربع run الذي يمكن الوصول له باستخدام مفتاح شعار ويندوز + حرف R في لوحة المفاتيح.

ما هو الوضع الطبيعي للمنافذ في الـ switch؟

Dynamic desirable.

الـ ipv6 كم يمثل بت وما هي الميزة الي تفرقه عن الـ ipv4؟

يمثل ١٢٨ بت والميزة التي تفرقه عن الـ ipv4 يقوم بزيادة حجم العنوان من ٣٢ بت (معيار IPv4) إلى ١٢٨ بت.

بروتوكول الـ OSPF ما الغرض منه وما هي مميزاته؟

اختصار لـ Open Shortest Path First ويعني اختيار المسافة الأقصر أولاً وهو من بروتوكولات الـ routing (التوجيه) المشهورة جداً ويعتبر أقوى وأسرع من بروتوكول EIGRP لأن الـ interval time الخاص به ٣٠ ثانية بدلاً من ٩٠ ثانية في بروتوكول الـ EIGRP.

مميزاته:

- متاح لكل الشركات.
- يرسل المعلومات المحدثة فقط.
- يدعم ال vlsms وال classless subnetting مثل (/19 - /12 - /9).
- يعتمد على سرعة الكابل المتاح فيختار الطريق الأقصر.
- يدعم عدد غير محدود من ال routers.
- يقسم الشبكات إلى مناطق متعددة areas.
- يستخدم خوارزمية ديكسترا Dijkstra Shortest Path First لتحديد المسار الأقصر.

لماذا يستخدم بروتوكول الـ FTP منفذين للنقل؟

بعض البروتوكولات لها رقم واحد وبعضها لها رقمين للمنافذ واحد يكون مخصص للسيرفر والآخر مخصص لأجهزة الـ client.

المنفذ رقم ٢٠ من أجل نقل البيانات والمنفذ رقم ٢١ مسؤول عن نقل الأوامر.

ما الفرق بين المنفذ access والمنفذ trunk؟

عند تعريف المنفذ على وضع (Access) فيفهم الـ switch أن الجهاز الذي سيتصل بهذا المنفذ هو جهاز شخصي أو سيرفر.

أما وضع الـ (Trunk) فيعتبر الـ switch أن الجهاز المتصل بهذا المنفذ هو switch آخر سيقوم بتبادل الـ Vlans فإذا لم يجد switch ووجد جهاز شخصي سيقوم الـ switch تلقائيا بتحويله إلى (Access) مما يسبب بعض التأخير.

وأمنيا يفضل تحويل جميع منافذ المستخدمين إلى (Access) مع استخدام خاصية الـ port security لعدم السماح للموظف بجلب أي جهاز خارجي وتوصيله على الشبكة بدون علم المسؤولين عن الشبكة مما يسبب مخاطر كبيرة.

ما هو الـ VRF؟

هو اختصار لـ Virtual Routing Forwarding وهو أحد أهم المفاهيم التي تعمل بها الـ MPLS والتي يتوضح مفهومها من خلال مفهوم VRF.

وهو عبارة عن جدول توجيه منفصل داخل الـ router وباستخدام VRFs يمكن استخدام router واحد كأكثر من router بشكل افتراضي طبعاً.

من خلال الـ VRF يمكننا تقسيم layer 3 device ليظهر وكأنه عدة أجهزة وهذا يعني أنه لكل جزء منافذه الخاصة وأيضاً routing table الخاص به.

مبدأ الـ VRF شبيه بالـ VLAN لكن الـ VLAN تعمل على تقسيم أجهزة الـ switches (layer 2 devices) بينما الـ VRF يعمل على تقسيم أجهزة الـ routers (layer 3 devices).

بعبارة أخرى يمكن القول VRF تعني التوجيه الافتراضي وإعادة التوجيه.

ما هي الـ MPLS؟

هي التقنية المستخدمة لربط الشبكات المحلية مع بعضها البعض لتكوين الشبكات الواسعة (أو ربط الشبكات المحلية مع الشبكة الواسعة WAN) من أجل نقل البيانات وتعمل هذه التقنية في الطبقة الثانية Data Link Layer.

ما الفرق بين الـ router والـ switch layer 3؟

الـ switch layer 3 يحتوي على منافذ أكثر فيمكن جعل منافذه تعمل كـ router فيصبح لدينا العديد من المنافذ تعمل كـ default gateway.

الـ router طبعاً أفضل للربط خصوصاً عند الربط مع الشبكات الخارجية لأنه يحتوي على مواصفات أفضل ويدعم بروتوكولات أكثر بينما الـ switch layer 3 لا يدعم بعض الخصائص الموجودة في الـ router

في حال وجود أكثر من vlan كيف يمكن عمل اتصال بينهم؟

نستخدم ما يسمى inter vlan routing الذي يعمل على ربط العديد من الـ vlan المختلفة.

ما الفرق بين EIGRP وOSPF؟

EIGRP خاص بشركة Cisco ولكنه أصبح مفتوح المصدر عام ٢٠١٣ و OSPF هو بروتوكول عام.

EIGRP أسرع من الـ OSPF.

EIGRP يدعم تقريباً ١٠٠ router ولا يمكن أن يصل إلى ٢٥٥ routers إلا بتنفيذ تعليمات محددة داخله بينما الـ OSPF يدعم عدد لا محدود من الـ routers.

EIGRP multicast address is 224.0.0.10 and OSPF is 224.0.0.5 and 224.0.0.6.

جدول يوضح أرقام أغلب المنافذ المستخدمة

البروتوكول	رقم المنفذ
FTP	20 - 21
SSH	22
Telnet	23
SMTP	25
DNS	53
DHCP	67 - 68
TFTP	69
HTTP	80
SNMP	161
HTTPS	443

ما هو الـ Mail Exchange؟

هو بروتوكول بريد إلكتروني تم تطويره بواسطة Microsoft كبديل لـ POP3 وIMAP. في حين أن جميع البروتوكولات الثلاثة هي في الأساس طرق مختلفة للمستخدم لقراءة رسائل البريد الإلكتروني الخاصة به فإن بريد Exchange الإلكتروني يسمح أيضًا بتكامل أفضل لميزات البريد الإلكتروني الإضافية مثل جهات الاتصال والتقويمات المشتركة.

ما الفائدة من VTP وهل يمكن تفعيله في جميع الـ switches من شركات مختلفة أو فقط switches محددة؟

هو اختصار لـ Vlan Trunk Protocol وهو البروتوكول الذي يقوم بإدارة شبكات الـ Vlan في الـ switches التي تكون ضمن نطاق (domain) واحد.

فائدته:

لو كان لدينا أكثر من switch داخل الشبكة ونريد عمل vlans في كل switch فبدلاً من تطبيق إعدادات إنشاء الـ vlan في كل switch نقوم بتطبيقها فقط في switch واحد ونفعل بروتوكول الـ VTP وبالتالي سوف يتم إنشاء الشبكات على باقي الـ switches بشكل أوتوماتيكي (أي يتم نسخ هذه الشبكات عبر الـ trunk port إلى باقي الـ switches الأخرى).