



تصميم الشبكات

CECC815

المحاضرة 03

د. أحمد محمود أحمد



مخطط المحاضرة

- ❖ استخدام المنهجية (من الأعلى للأسفل) في تصميم الشبكات .
- ❖ منهجية التصميم.
 - مثال.
- ❖ تدقيق الشبكة الحالية أو تقييمها.
- ❖ استخدام أدوات التقييم.
- ❖ طبقات التصميم الهرمي للشبكات.
- ❖ اعتماد نهج الوحدات (Modular) في تصميم الشبكات.



استخدام المنهجية (من الأعلى للأسفل) في تصميم الشبكات

❖ إطار سيسكو SONA:

- سيسكو: **(SONA)** Service Oriented Network Architecture، معمارية الشبكة الموجهة بالخدمات.
 - يسهم اعتماد SONA في تعزيز المرونة ورفع الكفاءة ودعم عمليات الأعمال (business processes) ...إلخ.
- في نموذج SONA تُعدّ الشبكة العنصر المشترك الذي يربط جميع مكونات البنية التحتية لتقنية المعلومات ويُمكنها.

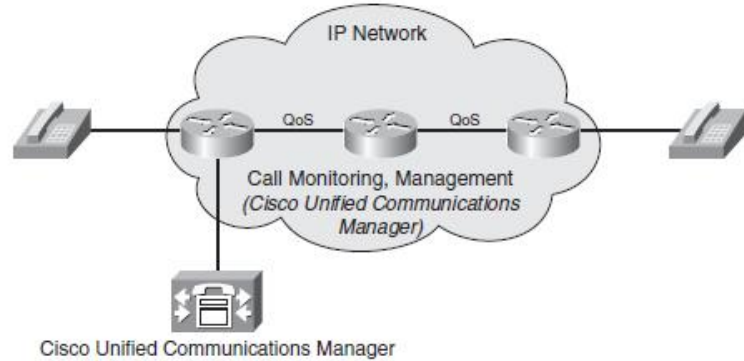


مثال على استخدام المنهج (من الأعلى للأسفل)

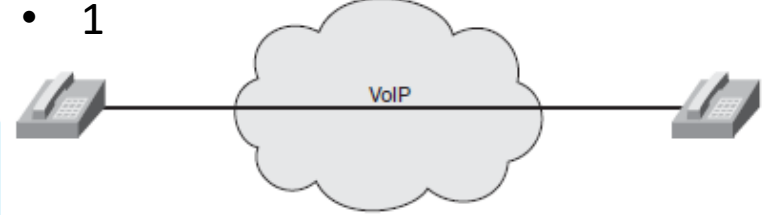
❖ تصميم حل لشبكة الهاتف عبر بروتوكول الإنترنت (IP Telephony).

▪ يتيح الهاتف عبر IP استخدام موارد الشبكة نفسها لنقل البيانات والصوت معاً، مما يخفض تكاليف تشغيل شبكتين منفصلتين.

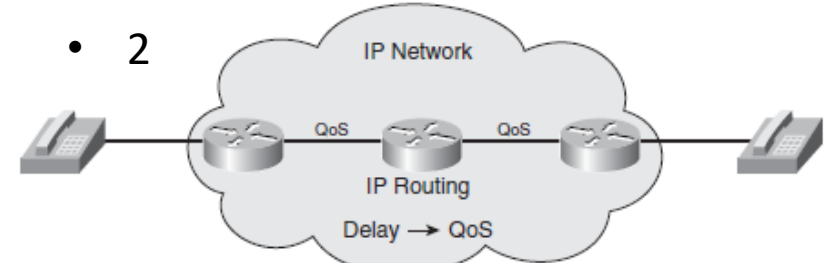
• 3



Cisco Unified Communications Manager Is Required for Monitoring and Managing VoIP Calls



A Voice over IP Network Is Required for IP Telephony



IP and QoS Are Required for VoIP



منهجية التصميم

- ❖ **المنهجية** هي طريقة موثقة ومنظمة للقيام بعملٍ ما.
- ❖ تتضمن منهجية التصميم ثلاث خطوات أساسية:
 - الخطوة 1: تحديد متطلبات العميل.
 - الخطوة 2: توصيف الشبكة الحالية والمواقع.
 - الخطوة 3: تصميم طوبولوجيا الشبكة والحلول.
- ❖ عند اكتمال التصميم تُنفَّذ عملية تطبيق التصميم، وتشمل الخطوات الآتية:
 - تخطيط عملية التنفيذ.
 - تنفيذ التصميم والتحقق منه.
 - المراقبة، وإعادة التصميم عند الحاجة.



منهجية التصميم / مثال

تقييم نطاق تصميم شبكة المؤسسة X

الملاحظات	نطاق التصميم
يتطلب العمود الفقري Backbone للشبكة في المكتب المركزي (الشبكة المركزية) (على فرض وجود شبكة مركزية و فروع بعيدة لها) إعادة تصميم. كما سَتُحدَّث الشبكات المحلية (LANs) في جميع الفروع إلى تقنية الإيثرنت السريع Fast Ethernet.	الشبكة بأكملها
يستلزم اعتماد عناوين IP خاصة وضع خطة عنوانية جديدة. كما ينبغي تقسيم بعض الشبكات المحلية (LANs) إلى مقاطع مستقلة. ويجب إعادة تصميم التوجيه (Routing) بما يدعم خطة العنوانية الجديدة ويوفر موثوقية أعلى وقدرًا أكبر من التكرارية.	طبقة الشبكة
يتطلب العمود الفقري في المكتب المركزي وبعض الفروع تجهيزات احتياطية، كما تقتضي الحاجة توفير وصلات احتياطية. وتحتاج المؤسسة أيضاً إلى مسح موقعي لترددات الراديو (RF) في الحرم المؤسسي لتحديد خيارات نشر التنقل اللاسلكي و المعدات المطلوبة.	طبقة ربط البيانات



منهجية التصميم / مثال

التطبيقات المخططة للمؤسسة X

نوع التطبيق	التطبيق	مستوى الأهمية (حرج، مهم، غير مهم)	الملاحظات
البريد الإلكتروني	Microsoft Office Outlook	مهم	
تطبيقات العمل الجماعي Groupware	Cisco Unified MeetingPlace	مهم	ضرورة إتاحة مشاركة العروض التقديمية والتطبيقات أثناء الاجتماعات عن بُعد.
تصفح الويب	Microsoft Internet Explorer، Opera، Netscape Navigator	مهم	
الفيديو عند الطلب Video on demand	Cisco Digital Media System	حرج	
قواعد البيانات	Oracle	حرج	تعتمد جميع عمليات تخزين البيانات على Oracle.
تطبيقات دعم العملاء	تطبيقات مخصصة	حرج	



منهجية التصميم / مثال

خدمات البنية التحتية المخططة للمؤسسة X

الملاحظات	الخدمة
يجب نشر منظومة الأمن على نحو منهجي، وذلك باستخدام تقنيات الجدار الناري لحماية الشبكة الداخلية، وتطبيقات فحص الفيروسات للتحقق من خلو حركة المرور الواردة من البرمجيات الضارة، وأنظمة كشف التسلل ومنعه IDS/IPS للحماية من محاولات الاختراق الخارجية المحتملة والتنبيه إليها. كما ينبغي النظر في استخدام أنظمة المصادقة والتفويض والمحاسبة (AAA) لضمان اقتصار الوصول إلى الخدمات المحددة على المستخدمين الموثقين والمصرح لهم.	الأمن (Security)
يتطلب الأمر تطبيق آليات جودة الخدمة (QoS) لإعطاء أولوية أعلى لحركة المرور الأهم والأشد حساسية للتأخير مقارنةً بالحركة الأقل أهمية، بحيث تُمنح أولوية أعلى لحركة الصوت وقواعد البيانات، وأولوية أدنى لحركة HTTP.	جودة الخدمة (QoS)
يستلزم الأمر إدخال أدوات مركزية لإدارة الشبكة وتركيبها، مثل HP OpenView مع تطبيقات CiscoWorks، بما يحقق إدارة أسهل وأكثر كفاءة أو أي أدوات أخرى.	إدارة الشبكة (Network Management)
ينبغي استخدام مسارات احتياطية وإنهاء الاتصالات على أجهزة شبكة مختلفة للقضاء على نقاط الفشل المفردة.	التوافر العالي (High availability)
يتطلب إدخال خدمات البث المتعدد عبر IP دعماً لتطبيقات مؤتمرات الفيديو وحلول التعلم الإلكتروني.	البث المتعدد عبر IP (IP multicast)
ترغب الشركة في الانتقال إلى الهاتفية المعتمدة على بروتوكول IP (IP telephony).	الصوت
توجد حاجة إلى خدمات التنقل للموظفين، وإلى إتاحة خدمة وصول الضيوف للعملاء.	التنقل (Mobility)

منهجية التصميم / مثال

الأهداف التنظيمية للمؤسسة X

الملاحظات	البيانات المجمعَة (الوضع الحالي)	الهدف التنظيمي
منتجات أفضل خفض التكاليف	المؤسسة Y المؤسسة Z	تعزيز القدرة التنافسية
نقطة إدخال بيانات واحدة تطبيقات سهلة التعلم تبادل بيانات بسيط	تكرار المهام، وإدخال البيانات مرات متعددة، ومهام تستغرق وقتاً طويلاً	خفض التكلفة
استحداث نظام ويب لتتبع الطلبات، وأدوات ويب للدعم الفني للعملاء	يتولى أفراد متابعة الطلبات وتقديم الدعم الفني	تحسين دعم العملاء
طلبات آمنة عبر الويب تأكيدات آمنة عبر الويب	الخدمات الحالية: طلبات عبر الهاتف والفاكس، وتأكيدات عبر الهاتف والفاكس	إضافة خدمات جديدة للعملاء



منهجية التصميم / مثال

القيود التنظيمية للمؤسسة X

الملاحظات	البيانات المجمعة (الوضع الحالي)	القيود التنظيمية
يمكن زيادة الميزانية (مقدار الزيادة) بحد أقصى قدره 78,000 دولار.	650,000 دولار	الميزانية
توجد خطط لتعيين مهندسين إضافيين لصيانة الشبكات، مع الحاجة إلى خطة تطوير تقني للعاملين.	مهندسان يحملان شهادات جامعية وشهادة مساعد شبكات سيسكو المعتمد (CCNA) لصيانة الشبكات؛ ويحمل أحدهما أيضاً شهادة محترف شبكات سيسكو المعتمد (CCNP). وثلاثة مهندسين لصيانة أنظمة التشغيل والتطبيقات المختلفة.	الكادر البشري
التجهيزات الحالية من Cisco، وهناك تفضيل للاستمرار معها.	تفضيل مورد واحد وبروتوكولات موحدة	السياسة
من التطبيقات التي سيجري إدخالها قريباً: مؤتمرات الفيديو، وتطبيقات العمل الجماعي، والهاتفية المعتمدة على بروتوكول IP.	توجد خطط لإدخال تطبيقات جديدة متنوعة خلال الأشهر التسعة المقبلة	الجدول الزمني



منهجية التصميم / مثال

الأهداف التقنية للمؤسسة X

الملاحظات	الأهمية	الأهداف التقنية
مهم في الموقع المركزي، وأقل أهمية في المكاتب الفرعية.	20	الأداء (Performance)
يجب أن تكون معاملات البيانات الحرجة آمنة.	15	الأمن (Security)
ينبغي أن تبلغ 99.9%.	25	الإتاحة (Availability)
	10	القدرة على التكيف (مع التقنيات الجديدة) (Adaptability)
يجب أن تكون الشبكة قابلة للتوسع.	25	قابلية التوسع (Scalability)
	5	قابلية الإدارة (Manageability)
	المجموع 100	



منهجية التصميم / مثال

القيود التقنية للمؤسسة X

الملاحظات	البيانات المجمعة (الوضع الحالي)	القيود التقنية
يجب استبدال منظومة الكابلات بكابلات الزوج المجدول Twisted paire حتى نقاط الوصول المكتبية، واستخدام الألياف الضوئية FO في الوصلات الصاعدة وفي العمود الفقري للشبكة.	كابل محوري (Coaxial Cable)	المعدات القائمة
ينبغي ترقية عرض الحزمة والانتقال إلى مزود خدمة آخر، لأن المزود الحالي لا يملك وصلات أخرى يمكن تقديمها.	وصلة شبكة واسعة النطاق (WAN) بسرعة 64 كيلوبت/ثانية	عرض الحزمة المتوفر
يجب أن تدعم تجهيزات الشبكة الجديدة (IPv6).	تطبيقات قائمة على الإصدار السادس من بروتوكول الإنترنت (IPv6).	توافق التطبيقات (Application Compatibility)



تدقيق الشبكة الحالية أو تقييمها

❖ يوفر التدقيق تفاصيل مثل الآتي:

- قائمة بأجهزة الشبكة.
- مواصفات العتاد وإصداراته، وإصدارات البرمجيات على أجهزة الشبكة.
- إعدادات تهيئة أجهزة الشبكة (Configurations).
- مخرجات أدوات التدقيق (auditing tools) المختلفة للتحقق من التوثيق القائم واستكمالها.
- معدلات استخدام الوصلات ووحدة المعالجة والذاكرة في أجهزة الشبكة.
- قائمة بالمنافذ (Ports) والوحدات (modules) والفتحات (slots) غير المستخدمة في أجهزة الشبكة، لفهم مدى قابلية الشبكة للتوسّع.



استخدام أدوات التقييم

❖ أمثلة على الأدوات:

■ CiscoWorks, WhatsUp Professional, SNMPc, Cacti NetMRI, NetVoyant, AirMagnet Survey PRO, Spectrum Expert.

❖ تحليل حركة مرور الشبكة والتطبيقات:

■ ميزة التعرف على التطبيقات اعتمادًا على الشبكة (Cisco IOS Network-Based Application Recognition (NBAR))

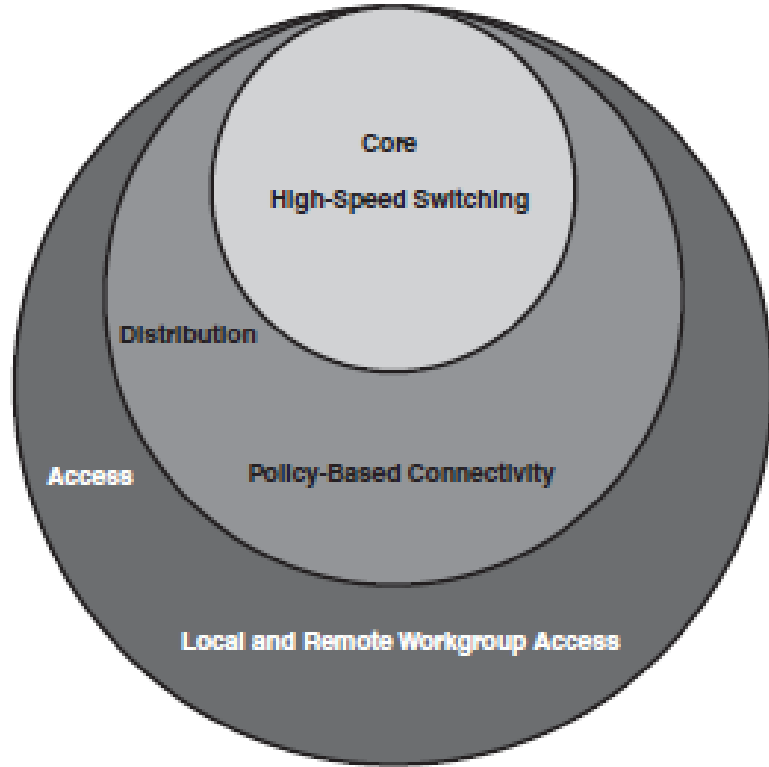
■ تقنية NetFlow في Cisco IOS.

■ يمكن لأداة SolarWinds Orion عرض معدلات الاستخدام.

■ يمكن لأداة Cacti عرض حركة المرور اليومية.



طبقات التصميم الهرمي للشبكات



Hierarchical Model's Three Layers

- ❖ يتكون نموذج التصميم الهرمي للشبكات من ثلاث طبقات:
- **طبقة الوصول Access layer:** توفر وصول مجموعات العمل أو المستخدمين إلى الشبكة محلياً وعن بُعد.
 - **طبقة التوزيع Distribution layer:** توفر اتصالاً قائماً على السياسات.
 - **طبقة النواة Core layer (أو العمود الفقري):** توفر نقلاً عالي السرعة لتلبية احتياجات الاتصال والنقل لأجهزة طبقة التوزيع.



وظائف طبقة الوصول (Access layer)

- ❖ تمثل نقطة التجميع التي ينفذ منها العملاء إلى الشبكة.
- ❖ وتهدف إلى منح المستخدمين إمكانية الوصول إلى موارد الشبكة.
- في بيئة الحرم الجامعي : عبارة عن أجهزة LAN (مُبدّلات) (Switches) بمنافذ تؤمّن اتصال محطات العمل والخوادم.
- في بيئة WAN: توفر وصول العاملين عن بُعد (teleworkers) إلى شبكة المؤسسة (الحرم الجامعي) عبر تقنيات واسعة النطاق WAN مثل Frame Relay و MPLS و ISDN والخطوط المؤجرة و DSL عبر الأسلاك النحاسية التقليدية للهاتف أو عبر كابل محوري.
- ولحماية سلامة الشبكة (network integrity): لا يُمنح الوصول إلا للمستخدمين أو الأجهزة الموثقين.



وظائف طبقة الوصول (Access layer)

- ❖ يمكن توفير الوصول للمستخدمين النهائيين ضمن بيئات تبديل من الطبقة الثانية (L2) أو ضمن بيئات التبديل متعدد الطبقات (L3).
- ❖ تشمل مهام طبقة الوصول:
 - تجميع المنافذ المُبدّلة 10/100 الخاصة بالمستخدمين.
 - توفير وصلات صاعدة Fast Ethernet و Fast EtherChannel و Gigabit Ethernet إلى طبقة التوزيع لتلبية متطلبات الاتصال وتقليل حجم نطاقات البث.
- ❖ **ملاحظة:** في الشبكات الصغيرة غالبًا ما تُدمج طبقة الوصول ضمن طبقة التوزيع.



وظائف طبقة التوزيع (Distribution layer)

- ❖ تمثل طبقة فصل بين طبقتي الوصول (Access) والنواة (Core)، ونقطة ربط بين مواقع الوصول المتنوعة وطبقة النواة.
- ❖ تحدد طبقة التوزيع صلاحيات وصول الأقسام أو مجموعات العمل، وتوفر **اتصالًا قائمًا على السياسات**.
 - الاتصال القائم على السياسات يعني تطبيق سياسات المؤسسة، مثل:
 - الترشيح (Filtering) بحسب عنوان المصدر أو الوجهة.
 - إخفاء أرقام الشبكات الداخلية عبر ترشيح المسارات (route filtering).
 - توفير مسارات ثابتة محددة بدلاً من الاعتماد على مسارات بروتوكول توجيه ديناميكي.
 - آليات الأمن وجودة الخدمة (QoS).



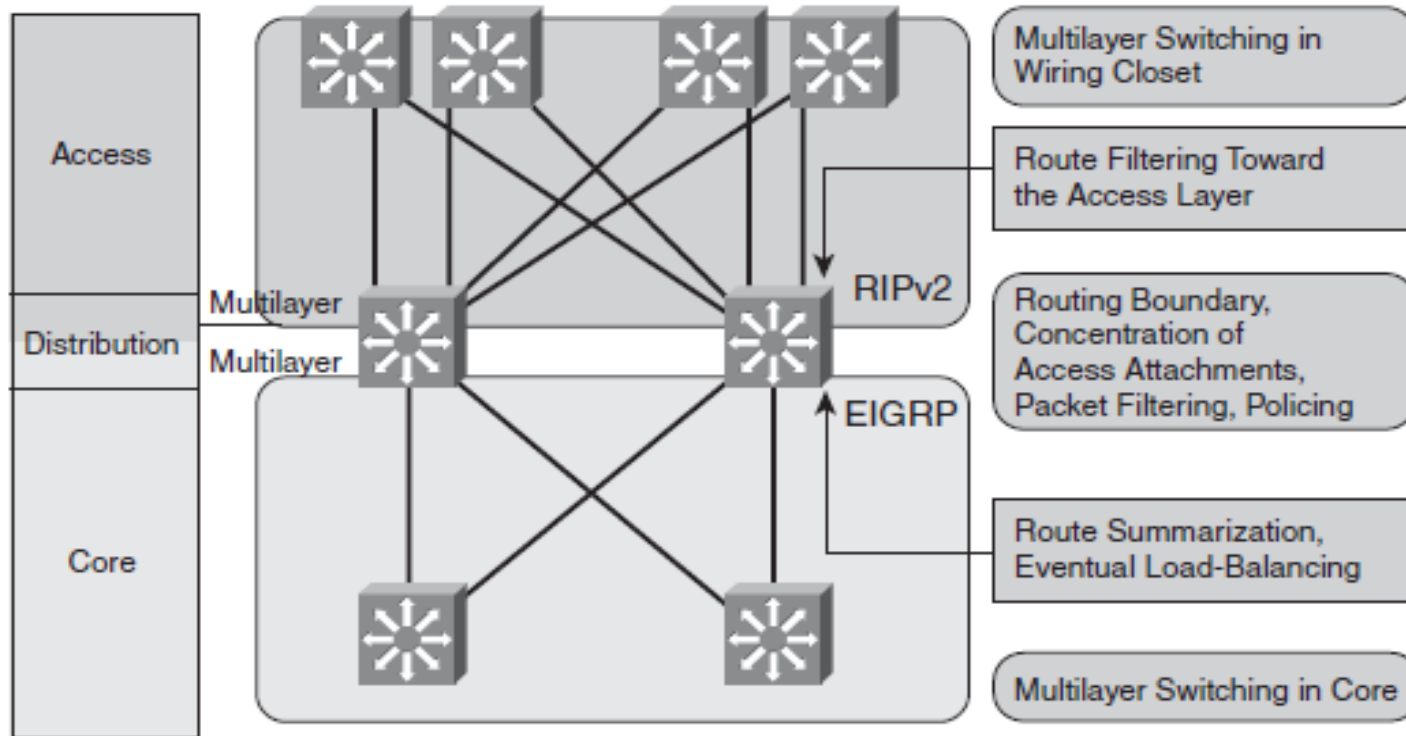
وظائف طبقة التوزيع (Distribution layer)

❖ من خصائص طبقة التوزيع:

- تتحكم أجهزة طبقة التوزيع في الوصول إلى الموارد المتاحة في طبقة النواة.
- في بيئة الحرم الجامعي، تجمع طبقة التوزيع سعة خزائن التوصيل (aggregates wiring closet bandwidth) عبر تركيز عدة وصلات وصول منخفضة السرعة في وصلة نواة عالية السرعة.
- في بيئة WAN تقوم بتجميع اتصالات WAN على أطراف الحرم الجامعي وتوفير اتصالاً قائماً على السياسات.
- توفر هذه الطبقة وصلات احتياطية لأجهزة الوصول (access devices).
- تمثل طبقة التوزيع حدًا للتوجيه بين طبقتي الوصول والنواة (Access) و (Core).
- يمكن لطبقة التوزيع تلخيص المسارات (**summarize routes**) القادمة من طبقة الوصول Access.



مثال على طبقة التوزيع (Distribution layer)



إعادة توزيع مسار ثنائي الاتجاه
two-way route redistribution

Example of Distribution Layer Features

شبكة حرم جامعي مُوجَّهة
routed campus network



وظائف طبقة النواة (Core layer)

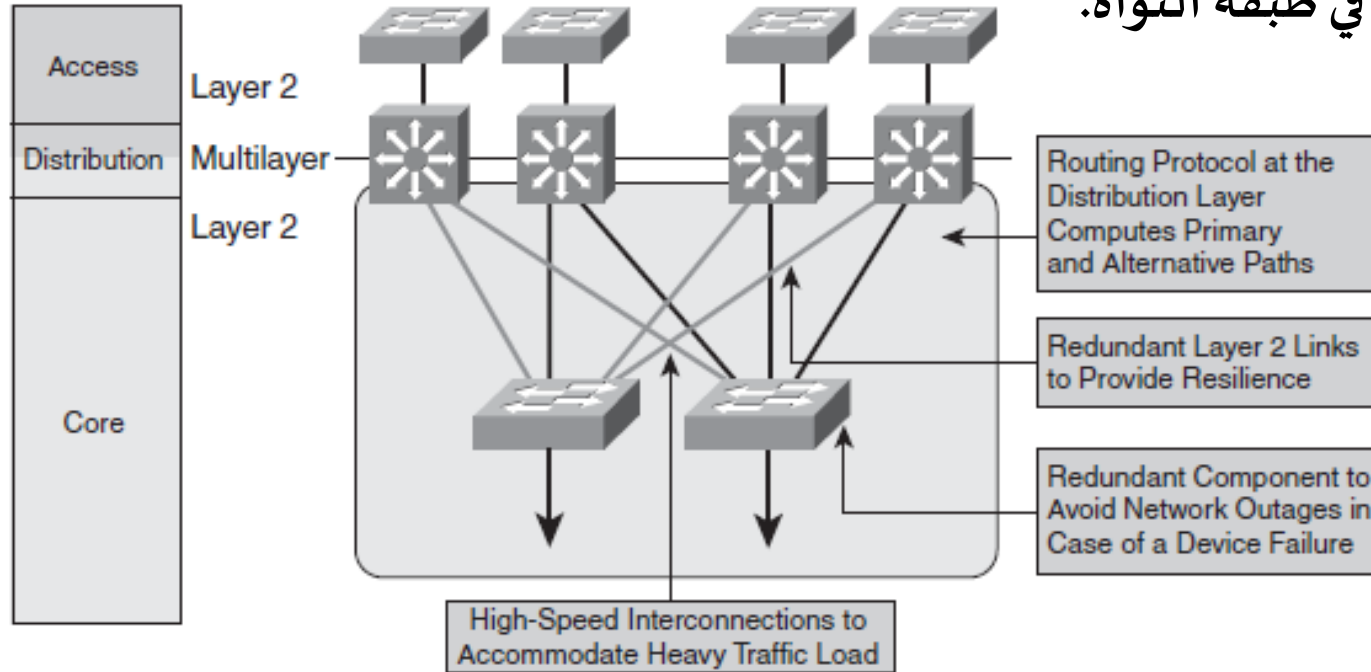
❖ تتمثل وظيفتها في توفير نقل بيانات سريع وفعال.

- طبقة النواة هي عمود فقري **عالي السرعة** ينبغي تصميمه لتمرير الحزم بأقصى سرعة ممكنة.
- ومن المتوقع أن توفر أجهزة طبقة النواة مستوى مرتفعاً من الإتاحة والاعتمادية (availability and reliability).
- ينبغي أن تحقق النواة درجة عالية من التكرار (redundancy) ، ويُوصى بشدة بالربط الشبكي الكامل (Full Mesh).
- **لا ينبغي لطبقة النواة إجراء أي معالجة للحزم** مثل فحص قوائم الوصول أو الترشيح (checking access lists or filtering)، لأن ذلك يبطئ عملية تمرير الحزم.
- كما يجب أن تكون طبقة النواة **قابلة للإدارة**.
- ويجب أن تدعم أجهزة النواة بروتوكولات وتقنيات قابلة للتوسع (scalable protocols and technologies)، وأن توفر مسارات بديلة وتوازناً في الأحمال (alternative paths and load balancing)



التبديل في طبقة النواة (Core layer)

❖ يمكن استخدام تبديل الطبقة الثانية أو التبديل متعدد الطبقات (التوجيه) في طبقة النواة، غير أن أغلب التطبيقات تعتمد التبديل متعدد الطبقات في طبقة النواة.

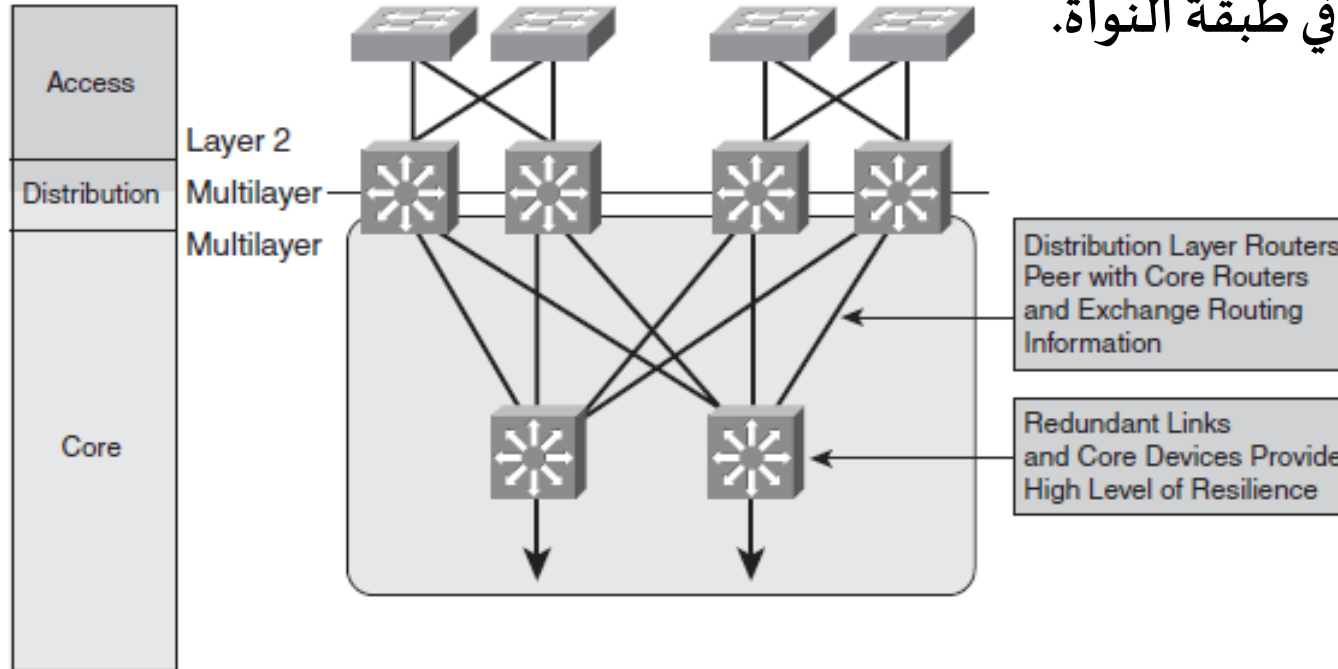


Layer 2 Switching in the Campus Core



التبديل في طبقة النواة (Core layer)

❖ يمكن استخدام تبديل الطبقة الثانية أو التبديل متعدد الطبقات (التوجيه) في طبقة النواة، غير أن أغلب التطبيقات تعتمد التبديل متعدد الطبقات في طبقة النواة.



Multilayer Switching in the Campus Core



اعتماد نهج الوحدات (Modular) في تصميم الشبكات

- ❖ نلاحظ هنا مفهوم الهرمية في:
 - الحرم الجامعي (طبقات الوصول والتوزيع والنواة)
 - شبكة WAN (يمثل المكتب البعيد remote office طبقة الوصول، والمكتب الإقليمي regional office يمثل طبقة التوزيع، والمقر الرئيسي headquarters يمثل طبقة النواة).
- ❖ تتيح الوحدات مرنة في تصميم الشبكة وتنفيذها وفي عمليات استكشاف الأعطال وإصلاحها.
- ❖ يرتبط إطار SONA لدى سيسكو بالوحدات الست في معمارية المؤسسة (Cisco Enterprise Architecture).
- **ملاحظة مهمة:** قد تظهر طبقات الوصول والتوزيع والنواة داخل كل وحدة من وحدات معمارية سيسكو للمؤسسة.

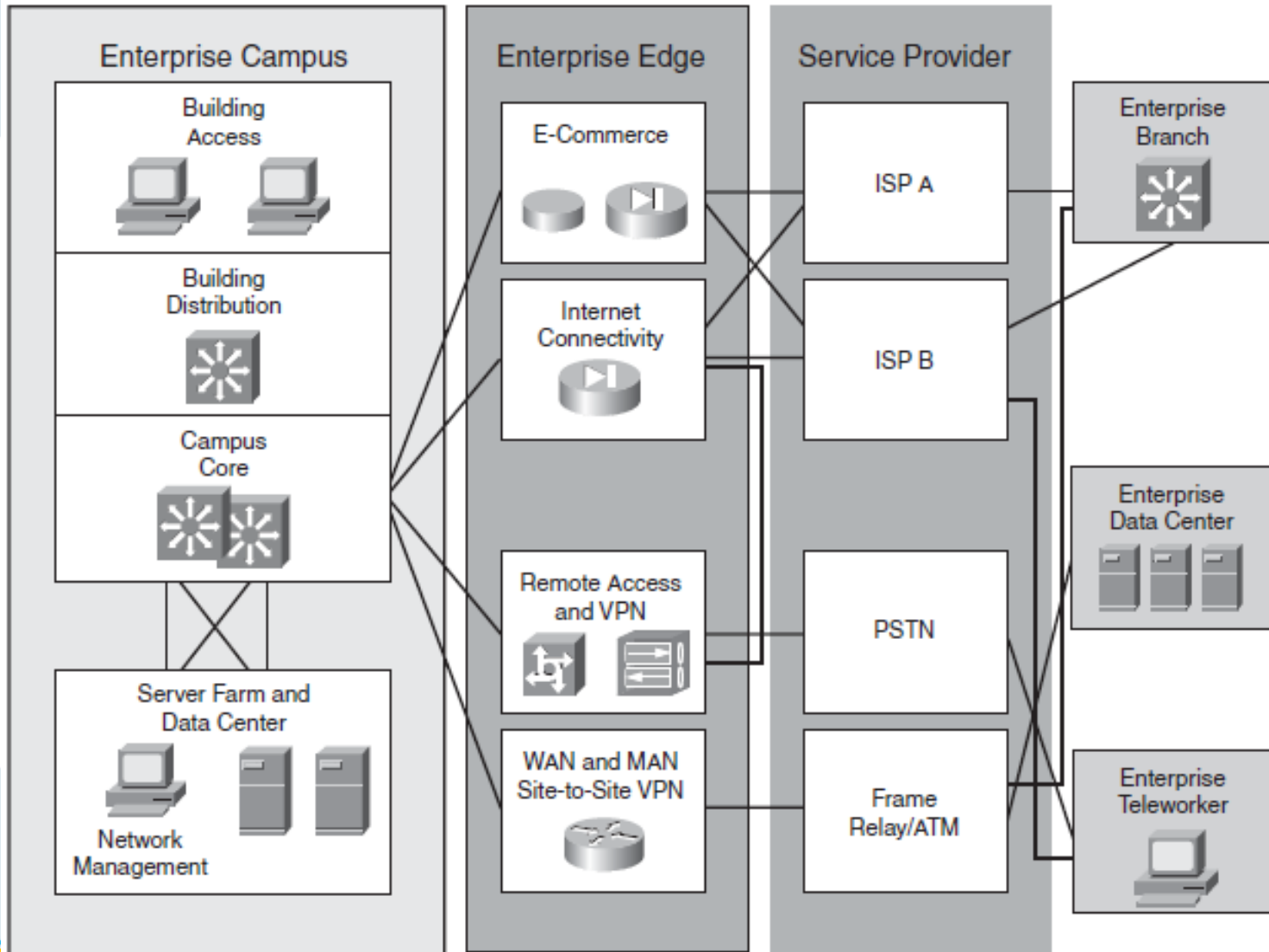


اعتماد نهج الوحدات (Modular) في تصميم الشبكات

❖ تتكون معمارية سيسكو للمؤسسة (Cisco Enterprise Architecture) من ستة مجالات وظيفية رئيسية (وتسمى أيضاً وحدات):

- حرم المؤسسة (Enterprise Campus): يشمل جميع الأجهزة والاتصالات داخل موقع الحرم الرئيسي.
- حافة المؤسسة (Enterprise Edge): تغطي جميع الاتصالات مع المواقع البعيدة والإنترنت من منظور حرم المؤسسة.
- مزود الخدمة (Service Provider).
- فرع المؤسسة (Enterprise Branch).
- مركز بيانات المؤسسة (Enterprise Data Center).
- الموظف عن بُعد (Enterprise Teleworker).

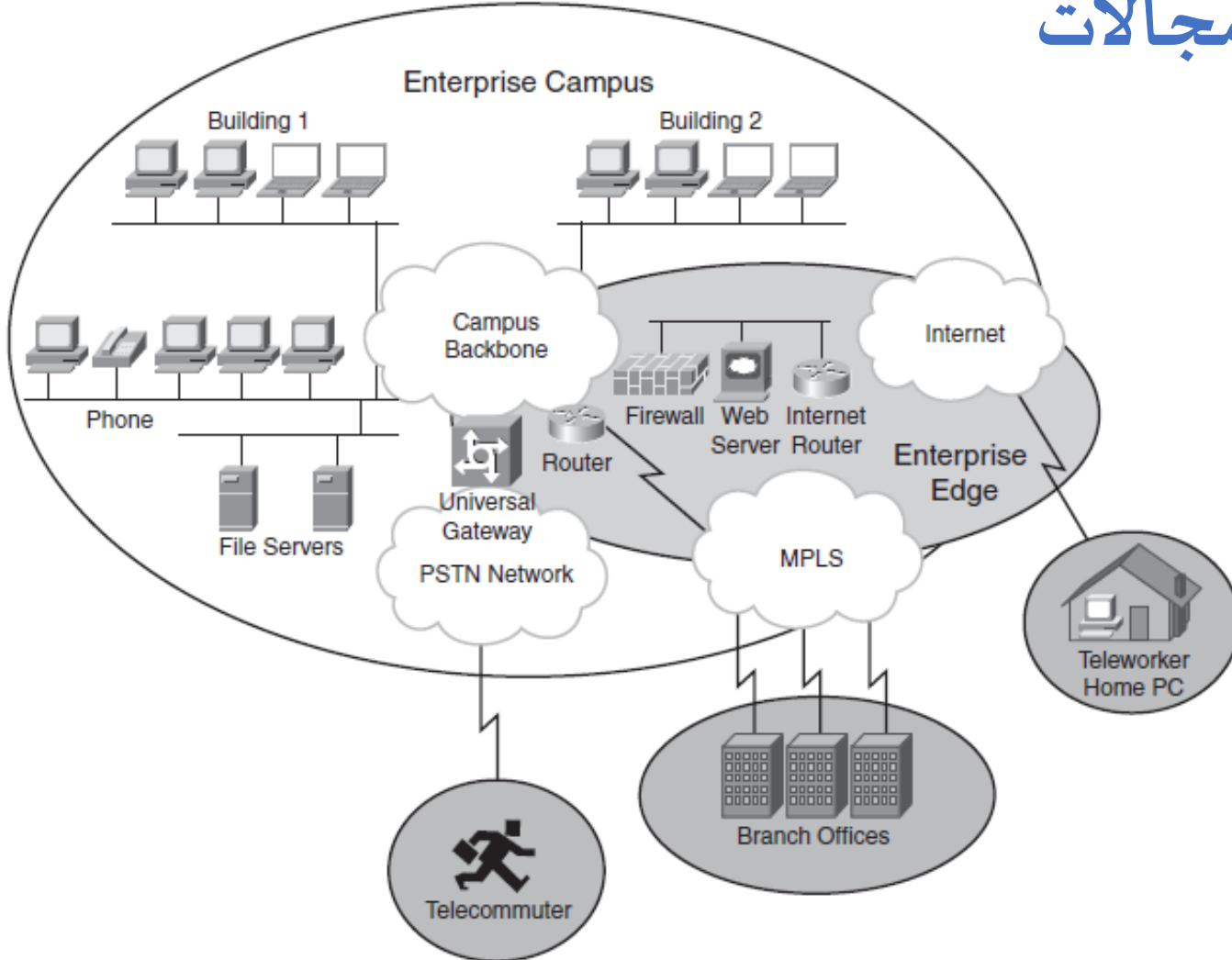




معمارية سيسكو للمؤسسة (Cisco Enterprise Architecture)



مثال لشبكة مقسمة إلى مجالات وظيفية



وحدات حافة المؤسسة (Enterprise Edge)

❖ يتكون مجال حافة المؤسسة من أربع وحدات رئيسية:

- وحدة التجارة الإلكترونية (E-commerce module): تتضمن الأجهزة والخدمات اللازمة لتمكين المؤسسة من تقديم تطبيقات التجارة الإلكترونية.
- وحدة اتصال الإنترنت (Internet Connectivity module): توفر لمستخدمي المؤسسة إمكانية الوصول إلى الإنترنت.
- وحدة الوصول عن بُعد وVPN (Remote Access and VPN module): تنهي حركة VPN والاتصالات الهاتفية الواردة من مستخدمي خارجيين.
- وحدة WAN وMAN وVPN بين المواقع (WAN and MAN and Site-to-Site VPN module): توفر الاتصال بين المواقع البعيدة والموقع المركزي عبر تقنيات WAN مختلفة.



وحدات حافة المؤسسة / وحدة التجارة الإلكترونية Enterprise Edge Modules/E-commerce Module

- ❖ لبناء حل تجارة إلكترونية ناجح، قد تتضمن الشبكة الأجهزة التالية:
 - خوادم الويب: واجهة المستخدم لتصفح خدمات التجارة الإلكترونية.
 - خوادم التطبيقات: تستضيف التطبيقات المختلفة.
 - خوادم قواعد البيانات: تحتوي معلومات التطبيق والمعاملات.
 - الجدران النارية أو موجّهات الجدار الناري: تنظّم الاتصالات وتوفر الأمن بين مستخدمي النظام المختلفين.
 - أجهزة كشف/منع التسلسل (NIDS/NIPS): تكشف الهجمات على الشبكة وتستجيب لها.
 - إلخ...



وحدات حافة المؤسسة / وحدة اتصال الإنترنت

Enterprise Edge Modules/Internet Connectivity Module

❖ تشمل المكونات الرئيسية المستخدمة في وحدة اتصال الإنترنت ما يلي:

- خوادم البريد (SMTP).
- خوادم نظام أسماء النطاقات (DNS).
- الخوادم العامة مثل FTP و HTTP والتي توفر معلومات عامة عن المؤسسة.
- الجدران النارية أو موجّهات الجدار الناري: توفر حماية على مستوى طبقة الشبكة للموارد، وتنفذ ترشيحًا متعلق بالحالة (Stateful filtering) لحركة المرور، وتُمرر حركة مرور بيانات VPN من المواقع والمستخدمين البعيدين حيث تنتهي جلسات VPN هنا.
- موجّهات الحافة: توفر ترشيحًا أساسيًا واتصالًا متعدد الطبقات مع الإنترنت.



وحدات حافة المؤسسة / وحدة الوصول عن بُعد Enterprise Edge Modules/Remote Access Module

❖ وحدة الوصول عن بُعد وVPN:

- تنهي حركة الوصول عن بُعد وحركة VPN (remote access traffic and VPN traffic) التي تقوم وحدة اتصال الإنترنت بتمريرها من المستخدمين والمواقع البعيدة.
- كما تستخدم وحدة اتصال الإنترنت لبدء اتصالات VPN مع المواقع البعيدة.
- كما تنهي الاتصالات الهاتفية (Dial-in) الواردة عبر شبكة الهاتف العامة (PSTN)، وبعد نجاح التوثيق تمنح المستخدمين إمكانية الوصول إلى الشبكة.



وحدات حافة المؤسسة / وحدة WAN و MAN و VPN بين المواقع (Site-to-Site)

- ❖ توجه حركة المرور بين المواقع البعيدة والموقع المركزي.
- ❖ وتستخدم تقنيات متنوعة مثل: الخطوط المؤجرة، و Frame Relay، و ATM، و PSTN، وشبكة SONET/SDH، والكابل، و DSL، و MPLS، و Metro Ethernet، واللاسلكي، وشبكات VPN التابعة لمزود الخدمة.



شكراً لحسن الاستماع هل من أسئلة؟

