



تصميم الشبكات

CECC815

المحاضرة 04

تصميم الشبكات المحلية (LAN)

د. أحمد محمود أحمد

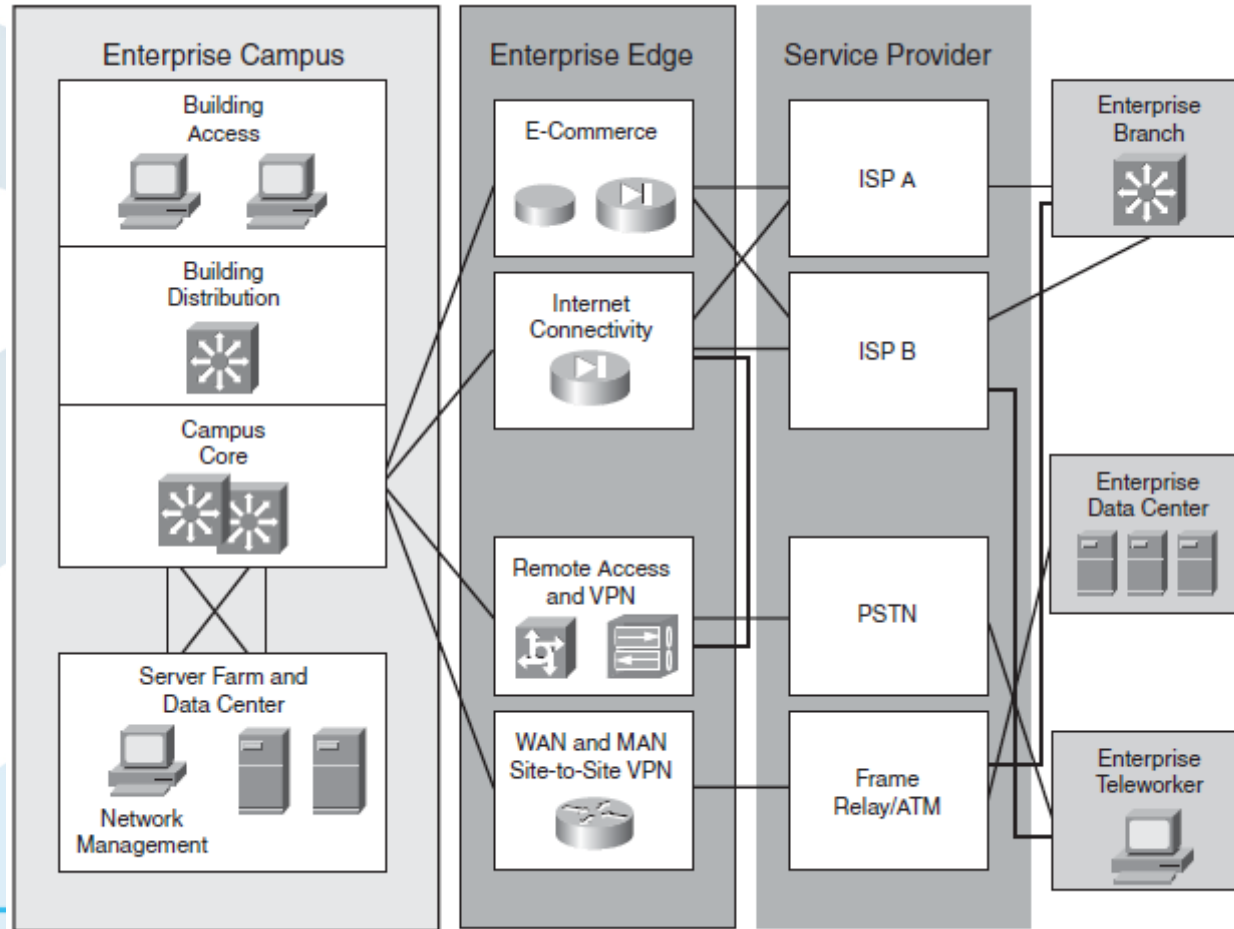


مخطط المحاضرة

- ❖ A day in the life: scenario
- ❖ Classless Interdomain Routing (CIDR)
- ❖ مثال
- ❖ معمارية المؤسسة من سيسكو (Cisco Enterprise Architecture)
- ❖ إرشادات تصميم حرم المؤسسة (Enterprise Campus Guidelines)
- ❖ إرشادات تصميم طرف المؤسسة (Enterprise Edge Guidelines)
- ❖ خدمات الأمن في التصميم الشبكي التجزيئي (Modular Network Design)
- ❖ تصميم التوافقية العالية في الشبكات
- ❖ خدمات الصوت في التصميم الشبكي التجزيئي (Modular Network Design)
- ❖ بروتوكولات وخصائص إدارة الشبكات
- ❖ اعتبارات تصميم شبكة الحرم



معمارية المؤسسة من سيسكو (Cisco Enterprise Architecture)



إرشادات تصميم حرم المؤسسة (Enterprise Campus Guidelines)

❖ **الخطوة 1:** اختيار الوحدات ضمن الحرم بحيث تماثل المباني وتضم طبقتي الوصول والتوزيع (access and distribution).

❖ **الخطوة 2:** تحديد مواقع وعدد مبدلات (Switches) طبقة الوصول، وتحديد وصلاتها الصاعدة نحو مبدلات طبقة التوزيع.

❖ **الخطوة 3:** اختيار مبدلات طبقة التوزيع المناسبة مع مراعاة عدد مبدلات طبقة الوصول والمستخدمين النهائيين، مع استخدام مبدلين على الأقل لضمان التكرارية (Redundancy).

❖ **الخطوة 4:** اعتماد وصلة صاعدة مزدوجة من كل مبدل وصول إلى مبدلي التوزيع.

❖ **الخطوة 5:** تحديد مواقع الخوادم، وتصميم وحدة (مزرعة الخوادم) (Server Farm) بحيث تضم مبدلين على الأقل في طبقة التوزيع لربط جميع الخوادم بتكرارية كاملة.

❖ **الخطوة 6:** تصميم طبقة قلب الحرم (Campus Core) ضمن وحدة بنية الحرم باستخدام مبدلين على الأقل بما يتناسب مع حجم الحركة المتوقعة بين الوحدات.

❖ **الخطوة 7:** ربط جميع وحدات حرم المؤسسة فيما بينها ضمن شبكة الحرم.



إرشادات تصميم طرف المؤسسة (Enterprise Edge Guidelines)

- ❖ **الخطوة 1:** إنشاء وحدة التجارة الإلكترونية (E-commerce): تطبيق سياسة أمنية عالية تتيح للعملاء الوصول إلى خوادم وخدمات محددة مسبقاً، وتقيّد أي عمليات أخرى.
- ❖ **الخطوة 2:** تحديد وصلات الربط بين شبكة المؤسسة (corporate network) والإنترنت، وإسنادها إلى وحدة اتصال الإنترنت (Internet Connectivity module): ينبغي أن تطبق هذه الوحدة ضوابط أمنية تمنع أي وصول غير مُصرّح به من الإنترنت إلى الشبكة الداخلية.
- ❖ **الخطوة 3:** تصميم وحدة الوصول البعيد (Remote Access) و VPN عند الحاجة، وتطبيق سياسة أمنية واضحة داخلها. تستخدم جلسات ال VPN لاتصال الذي توفره وحدة اتصال الإنترنت.
- ❖ **الخطوة 4:** تحديد الجزء من الطرف (edge) المخصّص حصراً للاتصالات الدائمة مع المواقع البعيدة (مثل الفروع) وإسناده إلى وحدة WAN و MAN و VPN موقع-إلى-موقع (Site-to-Site VPN module). تتموضع هنا جميع أجهزة ال WAN الداعمة ل ATM و Frame Relay والكوابل و MPLS والخطوط المؤجرة و SONET/SDH وغيرها.

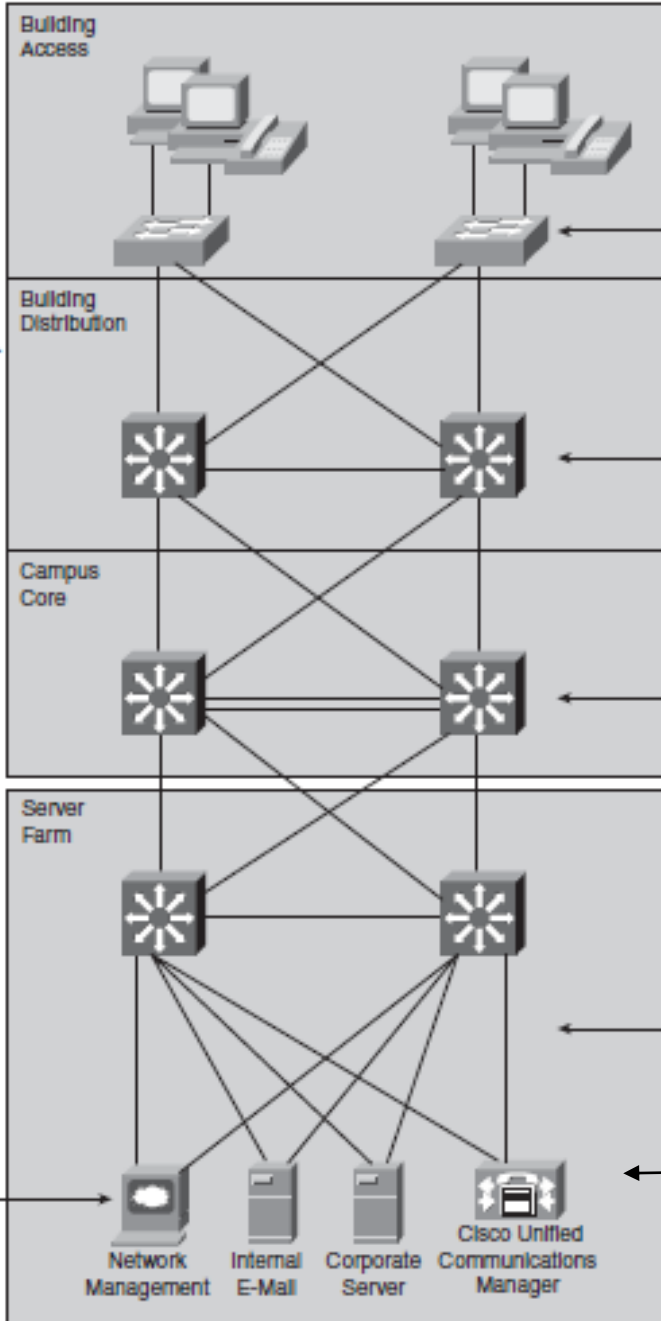


خدمات الأمن في التصميم الشبكي التجزيئي (Modular Network Design)

- ❖ تطبيق الأمن داخل حرم المؤسسة (Enterprise Campus) (أمن داخلي) وكذلك عند طرف المؤسسة (Enterprise Edge) لمواجهة التهديدات الخارجية.
- ❖ من الضروري أن تتضمن المؤسسة عدة طبقات حماية، بحيث لا يعني حدوث خرق في طبقة أو وحدة شبكية واحدة تعرّض بقية الطبقات أو الوحدات للاختراق.



خدمات الأمن في التصميم الشبكي التجزئي



استخدام أمن منافذ المبدل (switch port security) للتحكم في الوصول إلى الشبكة؛ إذ يتم التحكم في الوصول على مستوى المنفذ اعتماداً على معلومات طبقة ربط البيانات. مثل: الترشيح (filtering) اعتماداً على عنوان MAC ومصادقة المنفذ وفق معيار IEEE 802.1X

استخدام قوائم التحكم بالوصول (ACL) لتعزيز الأمن. ترشيح الحركة (filtering) بناءً على معلومات طبقة الشبكة وترشيح الحركة لمنع المرور غير الضروري عبر قلب الحزم.

عدم تنفيذ عمليات معالجة/تعديل الحزم في هذه الطبقة؛ إذ لا ينبغي أن تنفذ وظائف أمنية هنا، لأن ذلك قد يُبطئ عملية تبديل (Switching) الرزم.

استخدام أنظمة كشف التسلل (IDS) على مستوى المضيف والشبكة وأنظمة منع التسلل (IPS)، و VLAN خاصة، و قوائم تحكم بالوصول، وآليات كلمات مرور آمنة.

مع تطبيق المصادقة والتفويض والمحاسبة (AAA) ضمن منظومة أمنية كما يمكن أن يتكامل خادم AAA مع خادم كلمات المرور لمرة واحدة (OTP) لتوفير مستوى أمني عالٍ لجميع المستخدمين المحليين والبعيدين. استخدام خوادم المصادقة و OTP و IPS والتسجيل (Logging) لتقليل المخاطر الأمنية إلى الحد الأدنى.



تصميم التوافقية العالية في الشبكات

❖ يمكن اعتماد الأنواع الآتية من التكرارية (redundancy) ضمن وحدات المؤسسة:

- تكرارية الأجهزة، بما يشمل تكرارية البطاقات والمنافذ (card and port redundancy).
- وصلات مادية احتياطية (Redundant physical connections) لمحطات العمل والخوادم (الحرجة).
- تكرارية المسارات (Route redundancy).
- تكرارية الوصلات (Link redundancy).
- تكرارية الطاقة (Power redundancy)، بما يشمل مزودات طاقة احتياطية ضمن أجهزة الشبكة وتغذية كهربائية احتياطية لبنية المبنى.



تصميم التوافقية العالية في الشبكات

❖ من وسائل تحقيق تكرارية الاتصال (connection redundant):

- وصلات مادية متوازية بين المحولات والموجهات.
- وصلات احتياطية ضمن LAN و WAN.

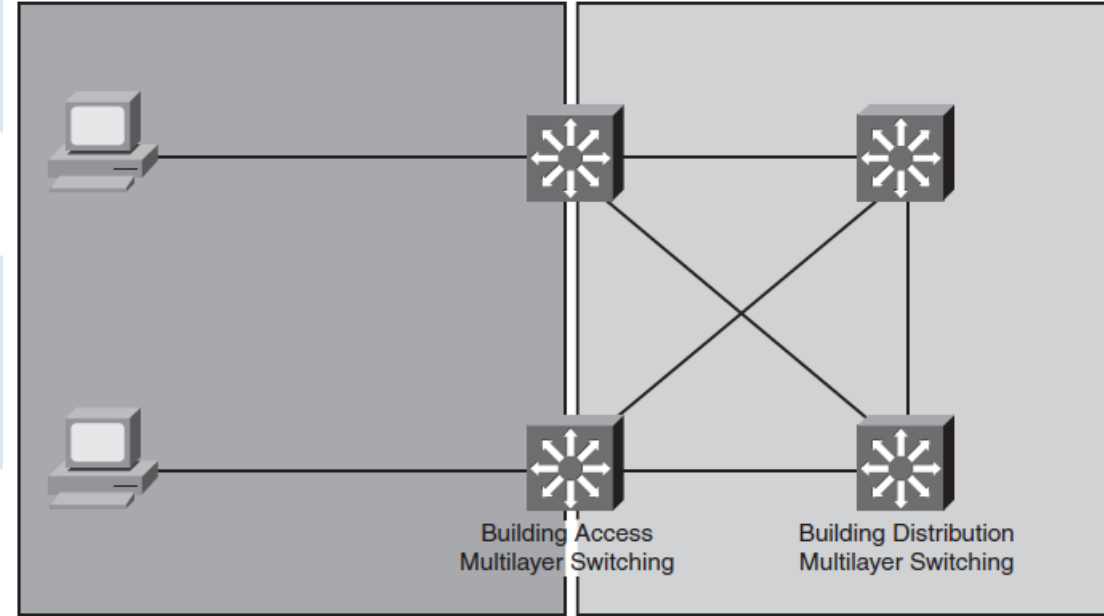
❖ ومن أساليب تكرارية الشبكة (network redundant):

- شبكة شبكية كاملة (Full Mesh) لتكرارية تامة وأداء مرتفع.
- شبكة شبكية جزئية (Partial Mesh) بتكلفة أقل وقابلية توسع أعلى.



تصميم التوافقية العالية في الشبكات

Campus Infrastructure Redundancy Example

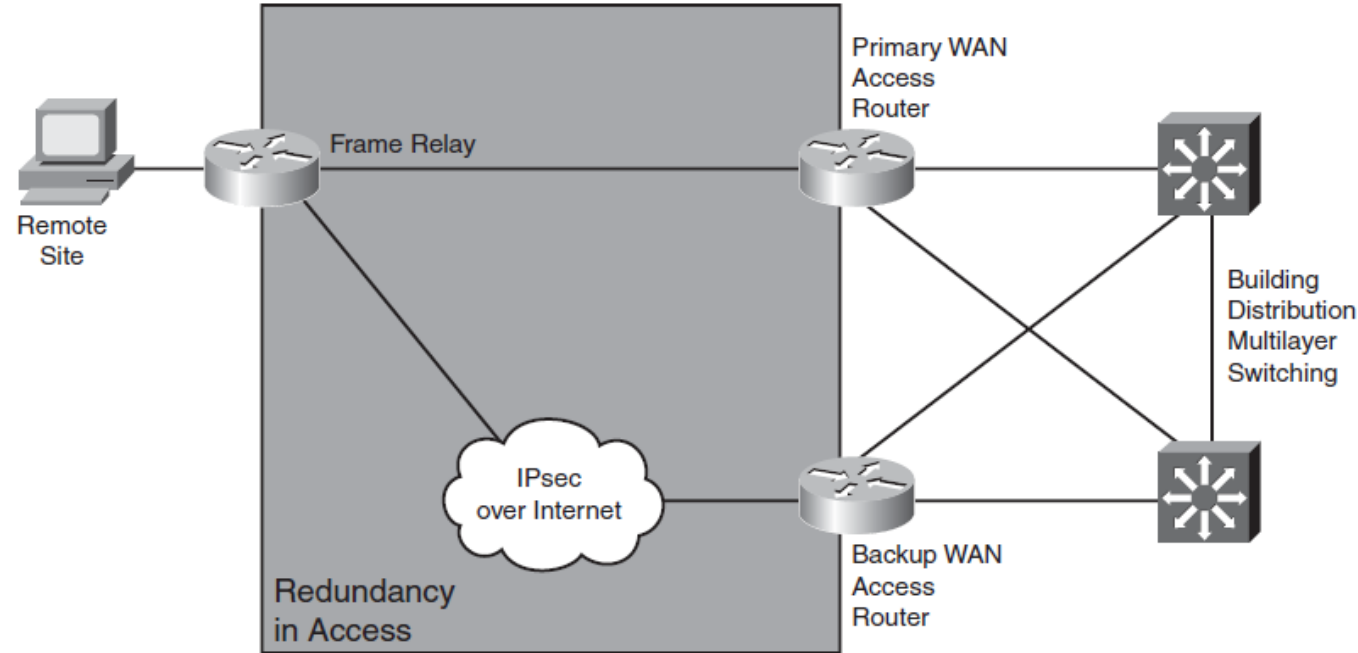


تختار المبدلات متعددة الطبقات المسارات الأساسية والاحتياطية بين طبقتي الوصول والتوزيع وفق قيمة المقياس (Metric) التي تحسبها خوارزمية بروتوكول التوجيه المستخدم.



تصميم التوافقية العالية في الشبكات

Example of Enterprise Edge Link Redundancy



غالباً ما تعتمد الوصلات الاحتياطية تقنية مختلفة؛ فمثلاً يمكن أن يقترن خط مؤجّر بوصلة IPsec احتياطية عبر الإنترنت.



خدمات الصوت في التصميم الشبكي التجزيئي (Modular Network Design)

❖ يمكن تقسيم نقل الصوت إلى ما يلي:

- VoIP: يعتمد على موجّهات داعمة للصوت، ويستخدم بروتوكول بدء الجلسة (SIP) للتحكم بالمكالمات والإشارة؛ وهو شفاف للمستخدمين.
- الهاتفية عبر IP (IP telephony): تعتمد على هواتف IP، وعلى خادم للتحكم بالمكالمات والإشارة مثل: (Cisco Unified Communications Manager).



مكوّنات الهاتفية عبر IP (IP telephony)

❖ الهواتف IP: تقوم بترميز الصوت وتحويله إلى حزم IP مع ضغطه باستخدام عتادٍ مخصص.

❖ المبدلات الداعمة لـ PoE: تمكّن من خلال الخزائن (wiring closet) من تزويد الهواتف IP بالطاقة ضمن الشبكات الهاتفية عبر IP.

- وهي شبيهة بالمبدلات التقليدية، لكنها تضيف خيار تزويد منافذ LAN بالطاقة حيث تُوصّل هواتف IP.
- كما تنفّذ بعض مهام جودة الخدمة (QoS) مثل تصنيف الحزم.

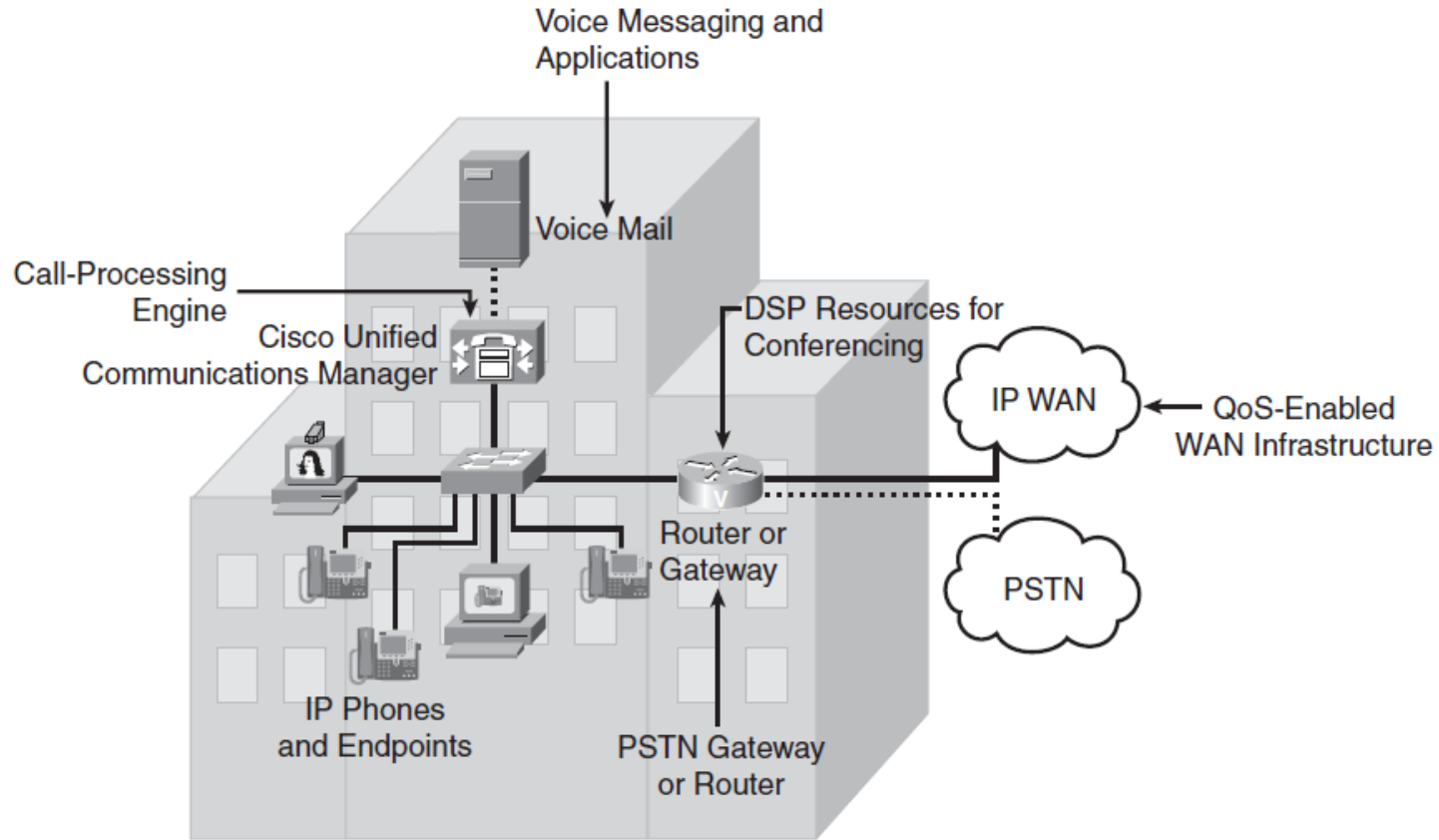
❖ مدير معالجة المكالمات: مثل Cisco Unified Communications Manager.

❖ بوابة الصوت (Voice gateway): وتُسمّى أيضاً موجّهات أو المبدلات الداعمة للصوت.



مكونات الهاتفية عبر IP (IP telephony)

IP Telephony Components

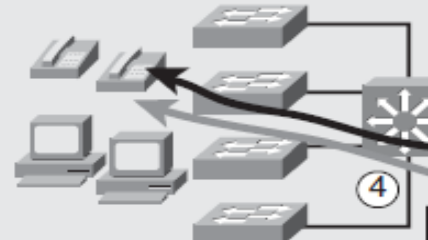


المنهج التجزيئي في تصميم شبكة الصوت

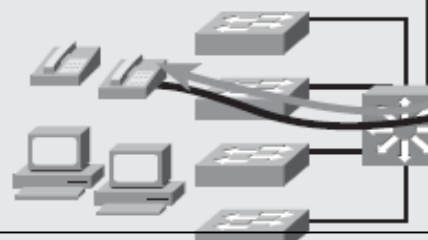
يتطلب تطبيق خدمات الصوت نشر خدمات حساسة للتأخير من طرف إلى طرف.

Voice Transport Example

Campus Infrastructure



IP Phone-to-IP Phone Session



جلسة طرف-إلى-طرف بين هاتفي IP

تأسيس الاتصال

Server Farm

Cisco Unified Communications Managers (2)

Dialing Plan:
-Local IP Phone
-Remote over IP WAN
-Remote over PSTN

Enterprise Edge

IP WAN

PSTN

المكالمات المتجهة إلى مواقع بعيدة. عبر وحدة WAN وMAN وVPN موقع-إلى-موقع، أو عبر وحدة الوصول البعيد وVPN.

تُمرّر المكالمات عبر طرف المؤسسة من خلال وحدة الوصول البعيد وVPN.



بروتوكولات وخصائص إدارة الشبكات

❖ تتكوّن معمارية إدارة الشبكات من:

- نظام إدارة الشبكات (Network management system - NMS).
- بروتوكول إدارة الشبكات (Network management protocol).
- الأجهزة المُدارة (Managed devices).
- وكلاء الإدارة (Management agents).



بروتوكولات وخصائص إدارة الشبكات

❖ يمتلك كل جهاز مُدار في الشبكة مجموعة متغيرات تعبر كمياً عن حالة الجهاز.

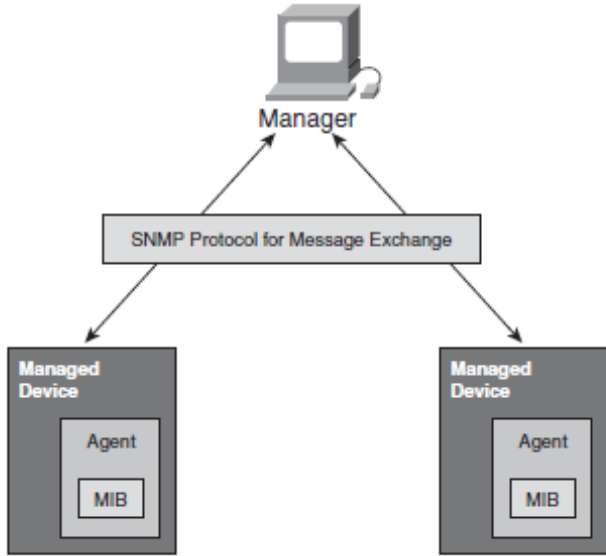
- يمكن مراقبة الأجهزة المُدارة عبر قراءة قيم هذه المتغيرات.
- كما يمكن التحكم بالأجهزة المُدارة عبر كتابة قيم جديدة لهذه المتغيرات.

❖ أصبح البروتوكول (SNMP- Simple Network Management Protocol) معياراً عملياً شائعاً في حلول إدارة الشبكات.

- المراقبة عن بُعد (RMON- Remote monitoring)
- قواعد معلومات الإدارة (MIB- Management Information Bases)



SNMP (Simple Network Management Protocol)



❖ المصطلحات المستخدمة في SNMP تشمل:

- المدير (Manager).
- البروتوكول (Protocol).
- الجهاز المُدار (Managed device).
- وكلاء الإدارة (Agents).

❖ SNMPv1 :Trap ، Get Response ، Set Request ، Get Next Request ، Get Request

❖ SNMPv2 :إضافة نوع الرسالة GetBulk و InformRequest.

❖ SNMPv3 :تحسينات وميزات أمنية.



RMON

❖ يتيح معيار RMON مراقبة الحزم وأنماط الحركة ضمن مقاطع LAN.

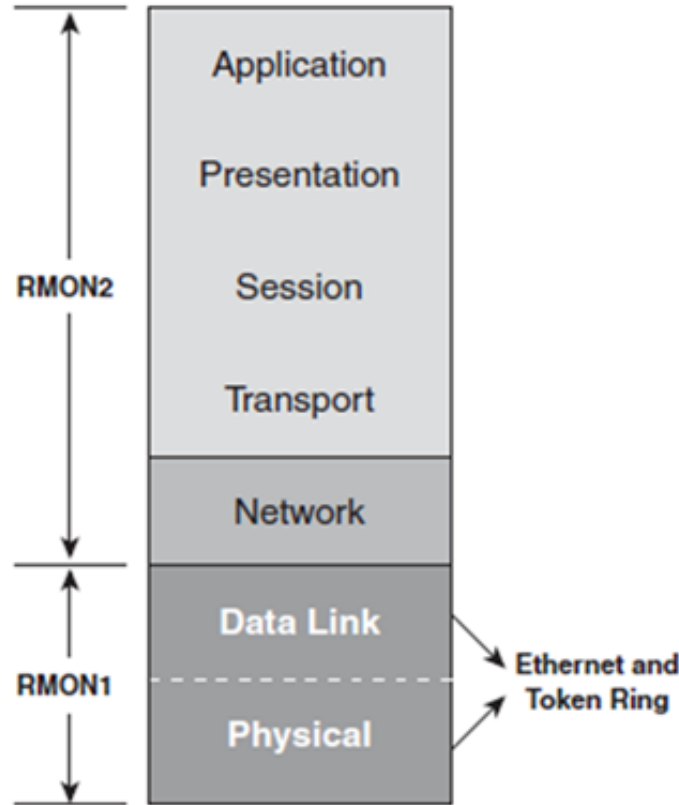
❖ يتتبع RMON العناصر الآتية:

- عدد الحزم.
- أحجام الحزم.
- رسائل البث (Broadcast).
- استغلال الشبكة (Network utilization).
- الأخطاء والظروف مثل تصادمات Ethernet.
- إحصاءات عن المضيفين (Statistics for hosts)، تشمل الأخطاء الصادرة عنهم، وأكثرهم انشغالاً، والمضيفين الذين يتواصلون فيما بينهم.



RMON

RMON2 Is an Extension of RMON1



❖ يعمل RMON1 على طبقة ربط البيانات بعناوين MAC ويقدم إحصاءات وتحليلاً إجمالياً لحركة LAN في المقاطع البعيدة.

❖ تم تطوير RMON2 لتوسيع الوظائف لتشمل بروتوكولات الطبقات الأعلى.

❖ **ملاحظات:**

■ Cisco NetFlow تقنية قياس تُسجّل التدفقات (Flows) التي تمر عبر أجهزة سيسكو.

■ CDP بروتوكول مملوك لسيسكو يعمل بين أجهزة سيسكو على طبقة ربط البيانات.

■ توفر خدمة رسائل Syslog وسيلة لتمكين النظام وعملياته من الإبلاغ بمعلومات حالة النظام إلى مدير الشبكة.



اعتبارات تصميم شبكة الحرم

❖ ينبغي مراعاة ثلاثة محاور رئيسية عند تصميم شبكة الحرم:

▪ خصائص تطبيقات الشبكة: الخدمات والتطبيقات ومتطلبات السعة وتأخير الإرسال.

▪ الخصائص البيئية:

• يؤثر الوسط الفيزيائي للمبنى أو المباني في قرارات التصميم،

• يُعدّ تمديد الكابلات من أكبر الاستثمارات طويلة الأجل في استمرارية الشبكات.

▪ خصائص أجهزة البنية التحتية: أثر خصائص أجهزة الشبكة المختارة في التصميم.



اعتبارات تصميم شبكة الحرم

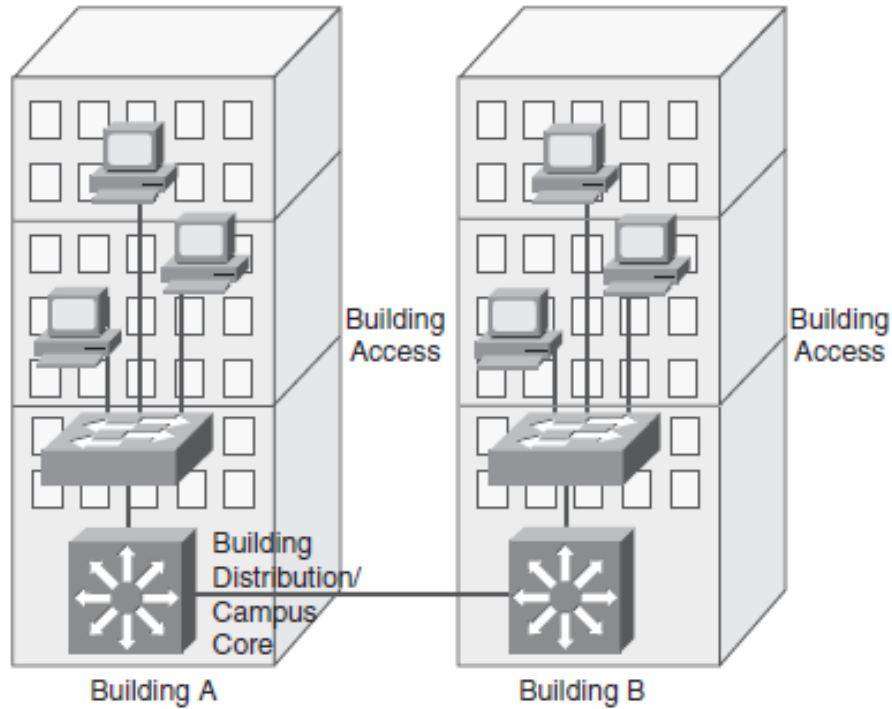
❖ خصائص تطبيقات الشبكة واعتباراتها:

- نداءً لندّ: (Peer-to-Peer):
 - ✓ المراسلة الفورية (Instant messaging).
 - ✓ مكالمات هواتف IP (IP phone calls).
 - ✓ مشاركة الملفات (File sharing).
 - ✓ أنظمة الاجتماعات المرئية (Videoconference systems).
- عميل/خادم: (Client-Server)
 - ✓ عميل - خادم محلي
 - ✓ عميل - مزرعة خوادم
 - ✓ عميل - خادم عند طرف المؤسسة (Edge server)



اعتبارات تصميم شبكة الحرم

Interbuilding Network Structure



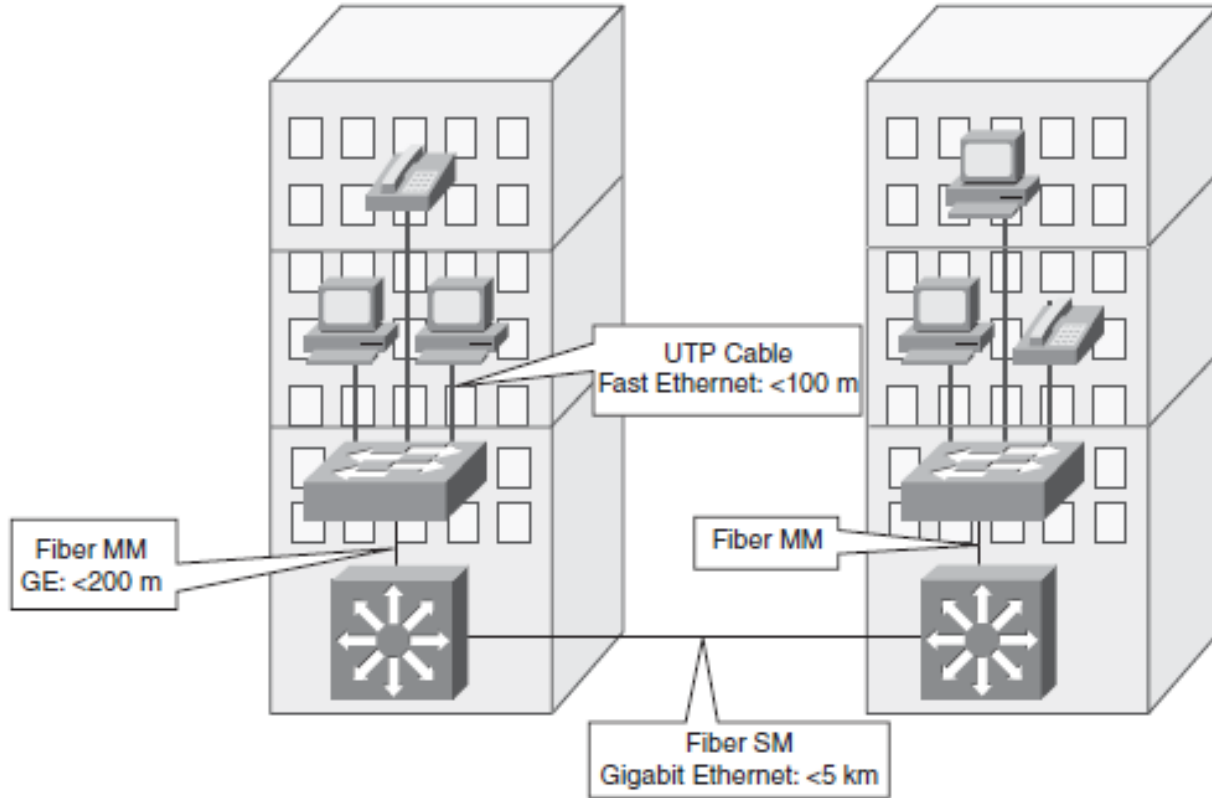
❖ الخصائص البيئية واعتباراتها:

- ضمن المبنى؟
- بين المباني؟
- مبنى بعيد/منفصل؟
- **ملاحظة:** المباني المتقاربة: تكون عادة على مسافات من بضع مئات الأمتار حتى بضعة كيلومترات.



اعتبارات تصميم شبكة الحرم

Campus Networks Use Many Different Types of Cables



❖ الخصائص البيئية واعتباراتها:

- مثال على التمديد بالكابلات
- صُممت الألياف الضوئية أحادية النمط (SMF) للاتصالات بعيدة المدى وعالية عرض الحزمة و السرعة باستخدام نواة ضيقة قطرها 9 ميكرومتر، بينما تُعد الألياف متعددة الأنماط (MMF) مثالية للتطبيقات قصيرة المدى (الشبكات المحلية، ومراكز البيانات) بنواة أعرض (50/62.5 ميكرومتر) وهي أرخص وأسهل في التوصيل للمسافات القصيرة.



اعتبارات تصميم شبكة الحرم

❖ خصائص أجهزة البنية التحتية واعتباراتها:

- عند اختيار نوع المبدل والخصائص المراد نشرها في الشبكة، تُؤخذ العوامل الآتية بالحسبان:
 - ✓ قدرات خدمات البنية التحتية: الخدمات التي تتطلبها المؤسسة مثل (IP Multicast و QoS وغيرها).
 - ✓ حجم مقاطع الشبكة: كيفية تقسيم الشبكة وعدد الأجهزة الطرفية المتوقع ربطها وفق خصائص الحركة.
 - ✓ زمن التقارب (Convergence): أقصى مدة قد تبقى خلالها الشبكة غير متاحة عند حدوث أعطال.
 - ✓ التكلفة: الميزانية المخصصة لبنية الشبكة التحتية.



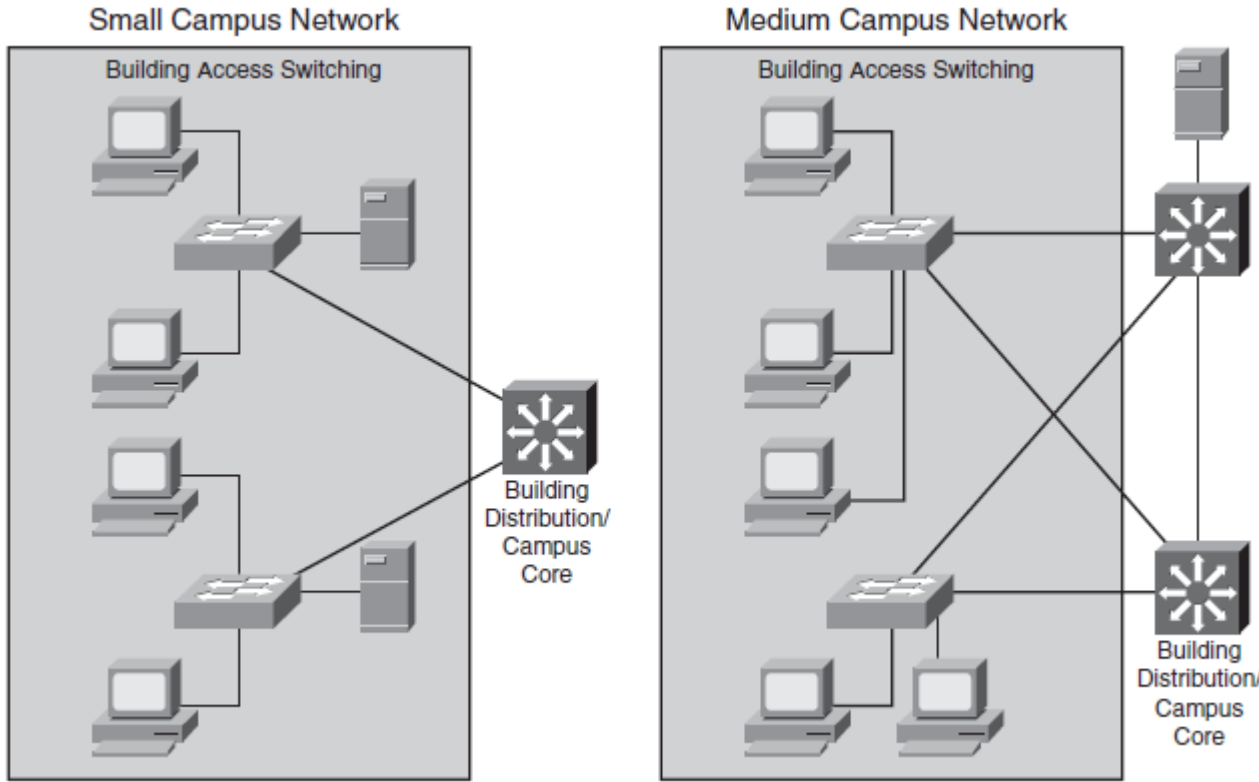
متطلبات حرم المؤسسة

Enterprise Campus Design Requirements

Requirement	Building Access	Building Distribution	Campus Core	Server Farm	Edge Distribution
Technology	Data link layer or multilayer switched	Multilayer switched	Multilayer switched	Multilayer switched	Multilayer switched
Scalability	High	Medium	Low	Medium	Low
High availability	Medium	Medium	High	High	Medium
Performance	Medium	Medium	High	High	Medium
Cost per port	Low	Medium	High	High	Medium



ملاحظات



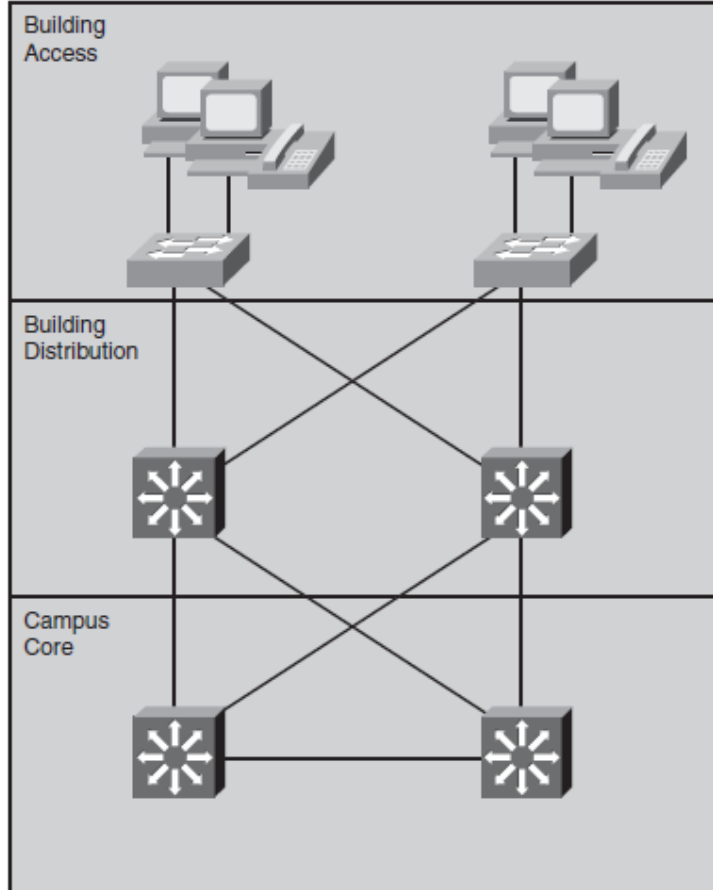
❖ شبكة حرم **صغيرة** (أو فرع كبير) قد تضم أقل من 200 جهاز طرفي.

❖ حرم **متوسط الحجم** يضم بين 200 و 1000 جهاز طرفي.



ملاحظات

Large Campus Multilayer Switched Campus Core Design



❖ عند تصميم **حرم كبير**، تكون طبقة قلب الحرم الأكثر مرونة وقابلية للتوسع عادة مكوّنة من محولين متعددي الطبقات يعملان بشكل مزدوج.

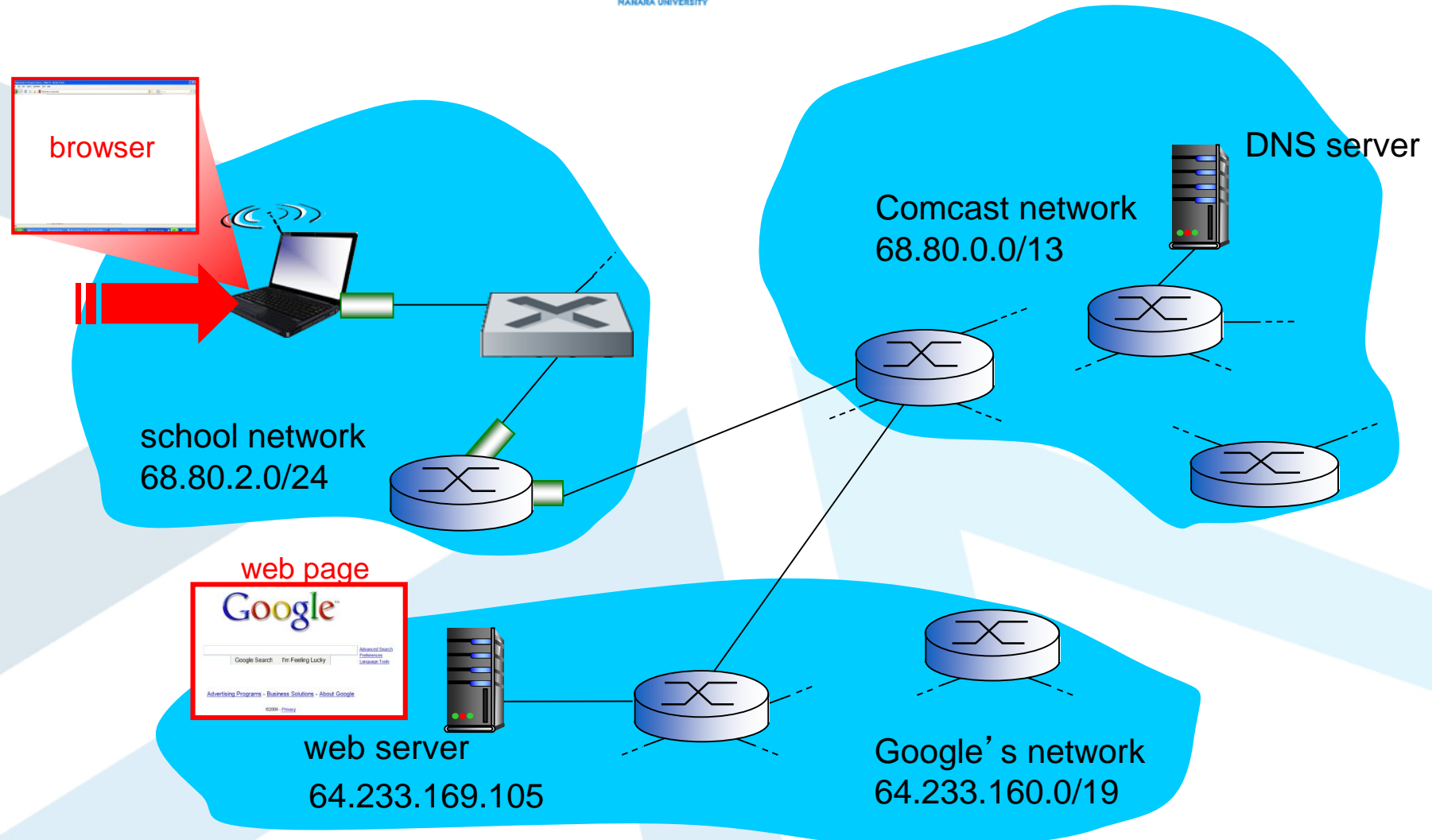


Synthesis: a day in the life of a web request

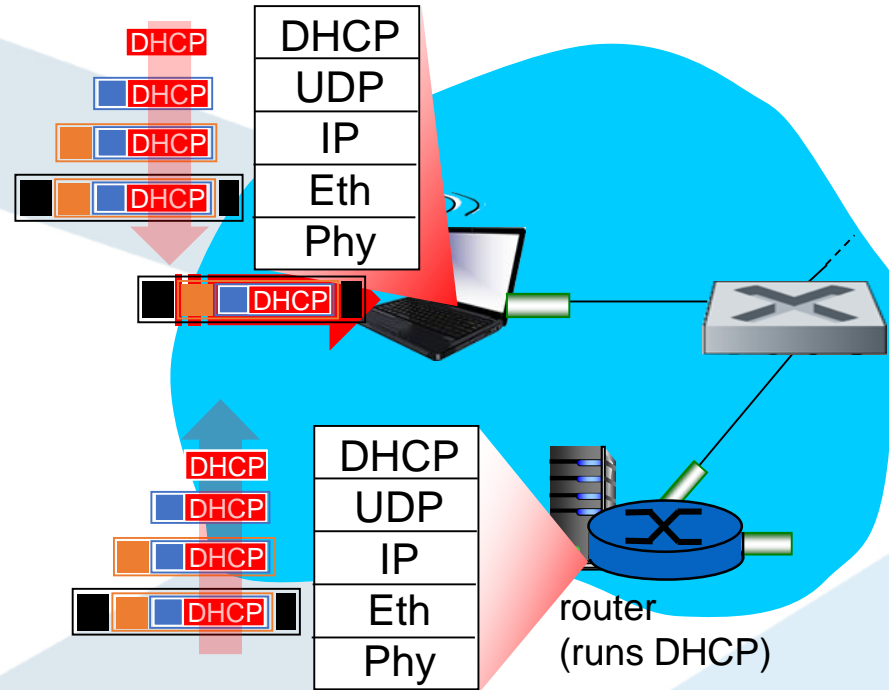
- journey down **protocol stack** complete!
 - application, transport, network, link
- putting-it-all-together: **synthesis!**
 - **goal**: identify, review, understand protocols (at all layers) involved in seemingly simple scenario: **requesting www page**
 - **scenario**: student attaches laptop to campus network, requests/receives **www.google.com**



A day in the life: scenario



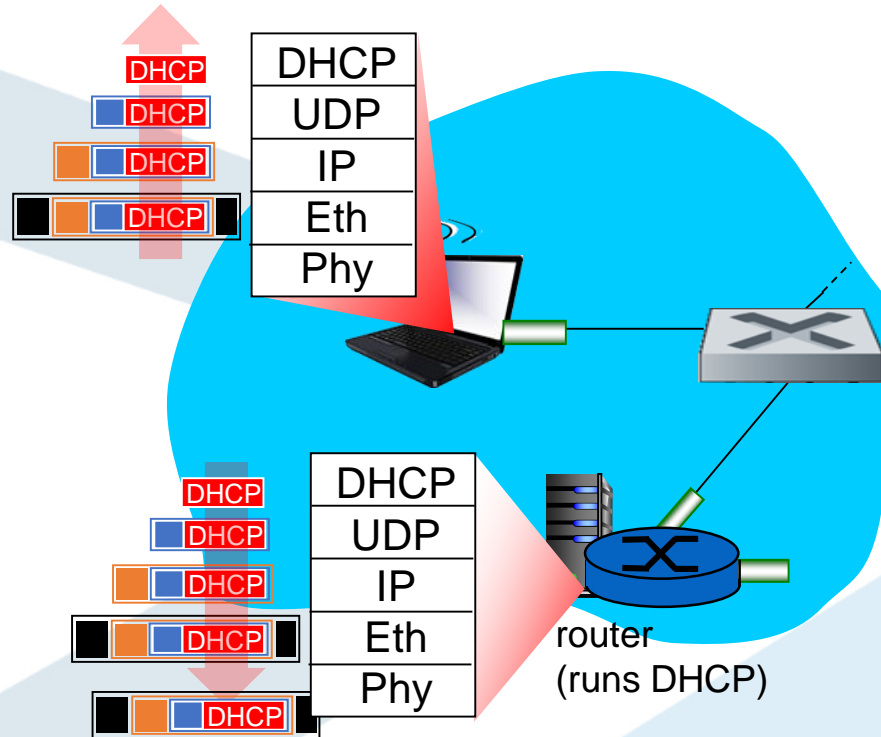
A day in the life: connecting to the Internet



- ❖ connecting laptop needs to get its own **IP address**, addr of **first-hop router**, addr of **DNS server**: use **DHCP**
- ❖ DHCP request **encapsulated** in **UDP**, encapsulated in **IP**, encapsulated in **802.3 Ethernet**
- ❖ Ethernet frame **broadcast** (dest: FFFFFFFFFFFFFFFF) on LAN, received at router running **DHCP** server
- ❖ Ethernet **demuxed** to IP demuxed, UDP demuxed to **DHCP**



A day in the life: connecting to the Internet

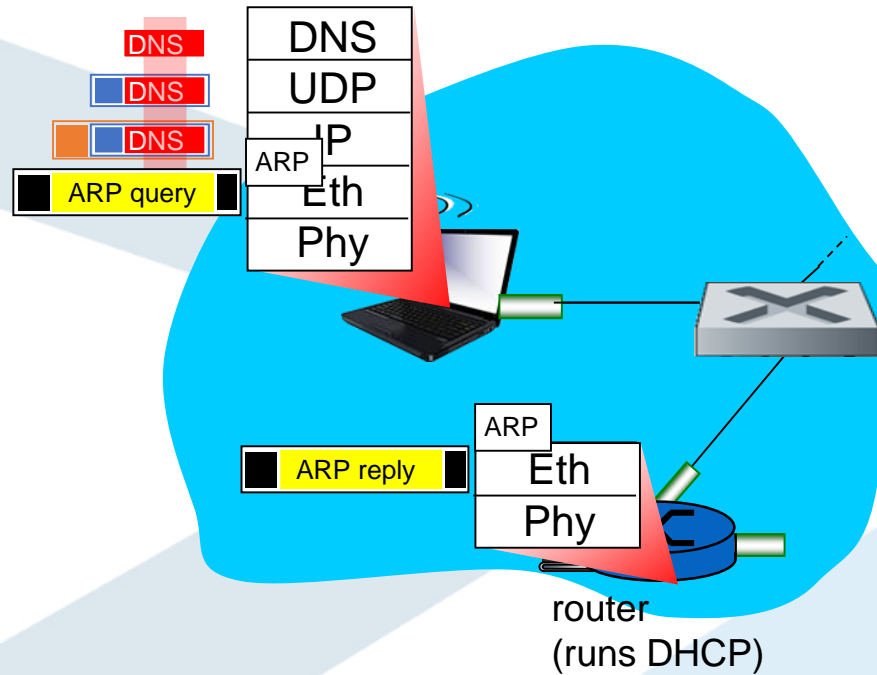


- DHCP server formulates *DHCP ACK* containing client's IP address, IP address of first-hop router for client, **name & IP address of DNS server**
- ❖ encapsulation at DHCP server, frame forwarded (**switch learning**) through LAN, demultiplexing at client
- ❖ DHCP client receives DHCP ACK reply

Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router



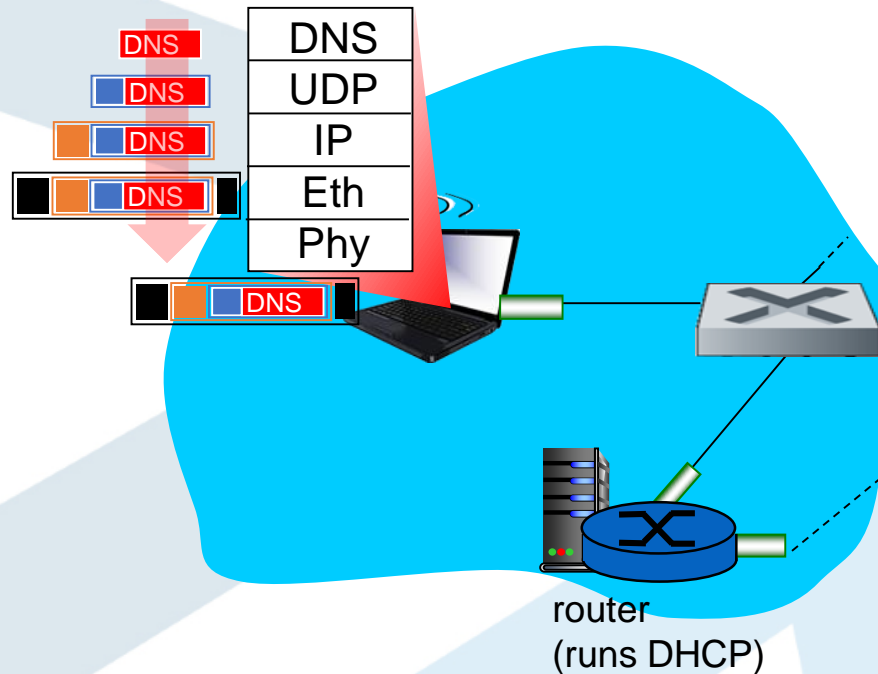
A day in the life: ARP (before DNS, before HTTP)



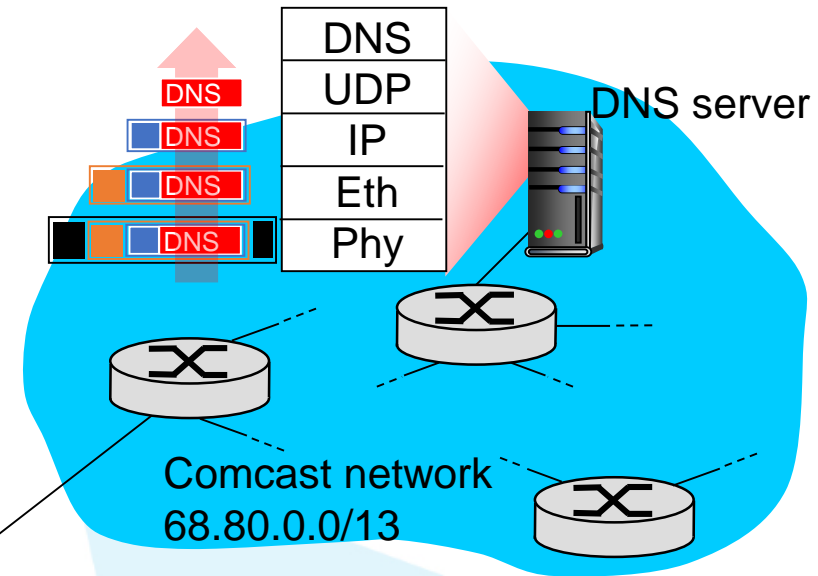
- ❖ before sending *HTTP* request, need IP address of `www.google.com`: *DNS*
- ❖ DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: *ARP*
- ❖ *ARP query* broadcast, received by router, which replies with *ARP reply* giving MAC address of router interface
- ❖ client now knows MAC address of first hop router, so can now send frame containing DNS query



A day in the life.... using DNS



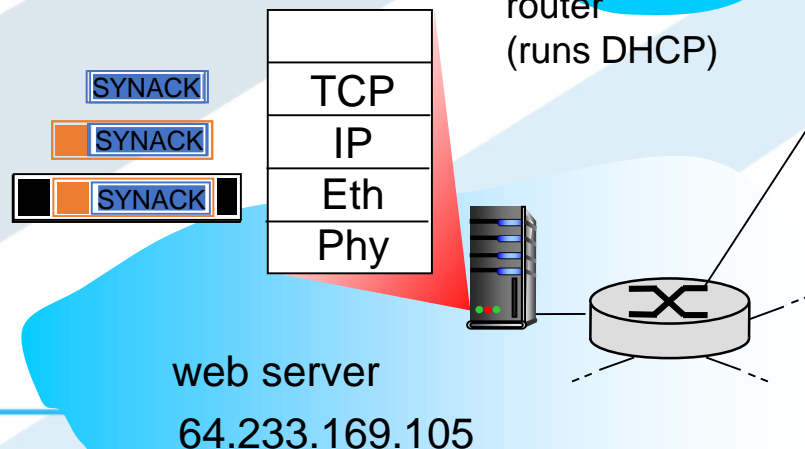
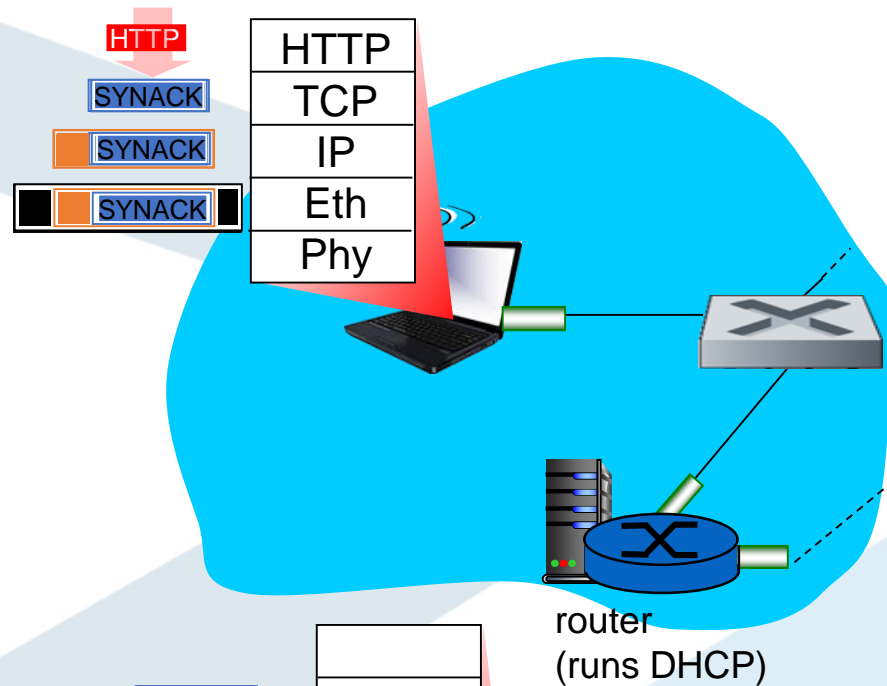
- ❖ IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router



- ❖ IP datagram forwarded from campus network into comcast network, routed (tables created by **RIP**, **OSPF**, **IS-IS** and/or **BGP** routing protocols) to DNS server
- ❖ demux' ed to DNS server
- ❖ DNS server **replies to client** with IP address of **www.google.com**



A day in the life.... TCP connection carrying HTTP

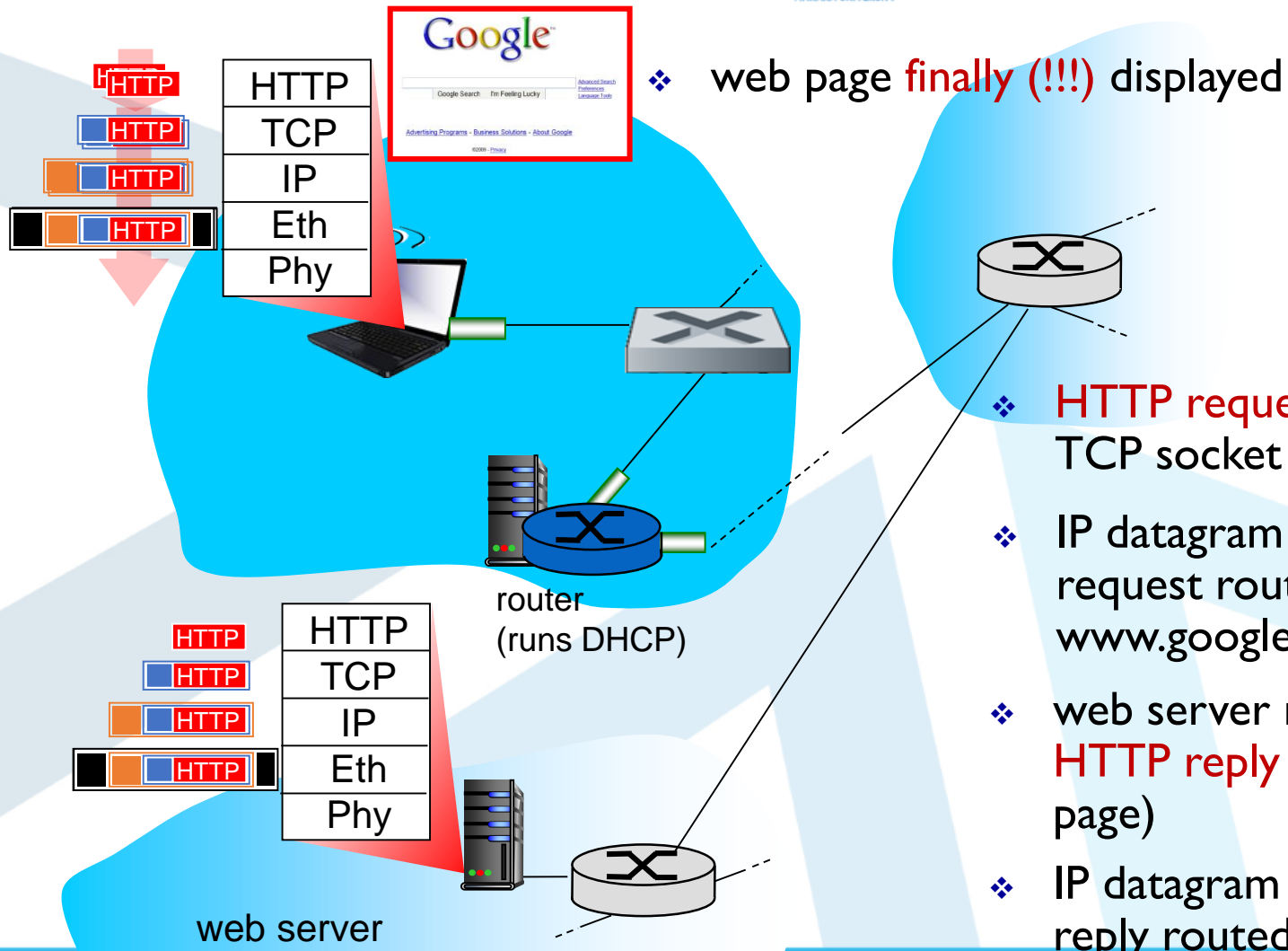


- ❖ to send HTTP request, client first opens **TCP socket** to web server
- ❖ TCP **SYN segment** (step 1 in 3-way handshake) **inter-domain** routed to web server
- ❖ web server responds with **TCP SYNACK** (step 2 in 3-way handshake)

❖ **TCP connection established!**



A day in the life..... HTTP request/reply



- ❖ web page **finally (!!!)** displayed
- ❖ **HTTP request** sent into TCP socket
- ❖ IP datagram containing HTTP request routed to **www.google.com**
- ❖ web server responds with **HTTP reply** (containing web page)
- ❖ IP datagram containing HTTP reply routed back to client



Classless Interdomain Routing (CIDR)

➤ **For example**, a router has the following networks behind it:

- 192.168.168.0/24
- 192.168.169.0/24
- 192.168.170.0/24
- 192.168.171.0/24
- 192.168.172.0/24
- 192.168.173.0/24
- 192.168.174.0/24
- 192.168.175.0/24

✓ Each of which could be **advertised separately**; however, this would mean advertising **eight routes**.



Classless Interdomain Routing (CIDR)

- Instead, this router can summarize the eight routes into one route and advertise 192.168.168.0/21.
- By advertising this one route, the router is saying, “Route packets to me if the destination has the first 21 bits the same as the first 21 bits of 192.168.168.0.”

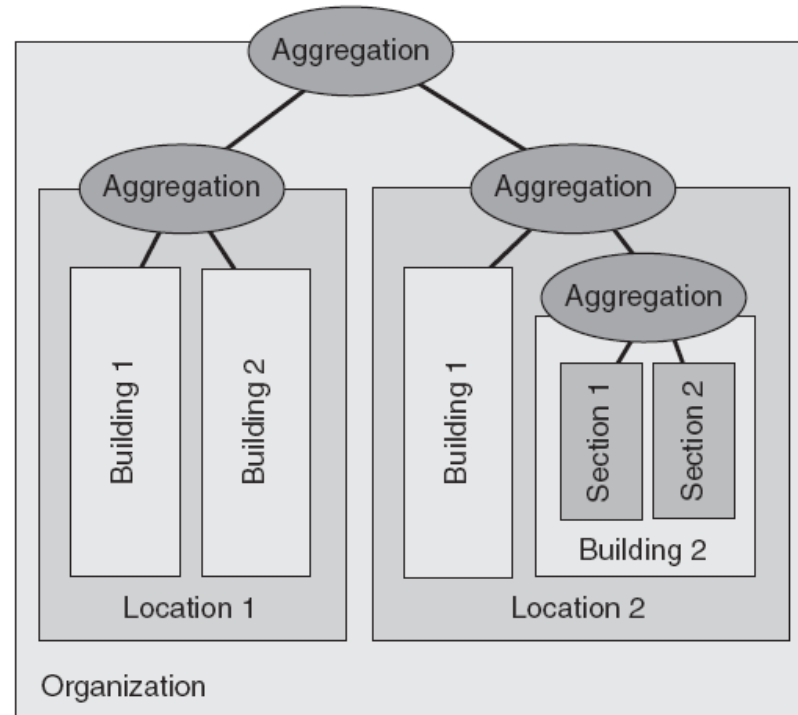
192.168.168.0 =	11000000 10101000 10101	000	00000000
192.168.169.0 =	11000000 10101000 10101	001	00000000
192.168.170.0 =	11000000 10101000 10101	010	00000000
192.168.171.0 =	11000000 10101000 10101	011	00000000
192.168.172.0 =	11000000 10101000 10101	100	00000000
192.168.173.0 =	11000000 10101000 10101	101	00000000
192.168.174.0 =	11000000 10101000 10101	110	00000000
192.168.175.0 =	11000000 10101000 10101	111	00000000

Number of Common Bits = 21
Number of Non-Common Network Bits = 3
Number of Host Bits = 8



Summarization Groups

- To reduce the routing overhead in a large network, a **multilevel hierarchy** might be required.
- The **depth** of hierarchy **depends on the network size** and the size of the highest-level summarization group.

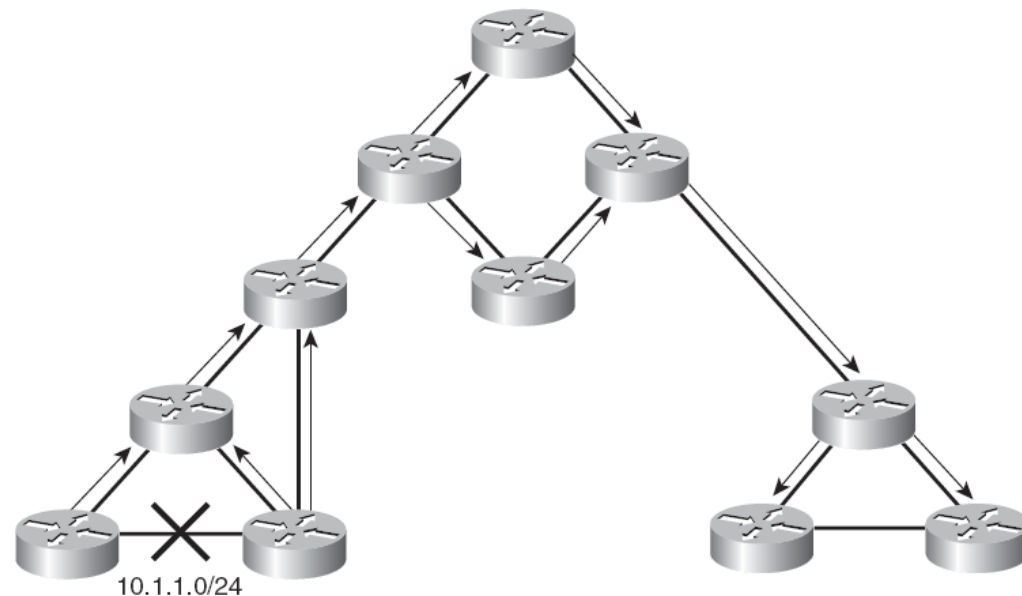


Impact of Poorly Designed IP Addressing

➤ Because aggregation is not applied, the routing update is **propagated throughout the entire network**, even if there is no need for a **distant router** to have detailed knowledge of that link.

➤ Impacts include the following:

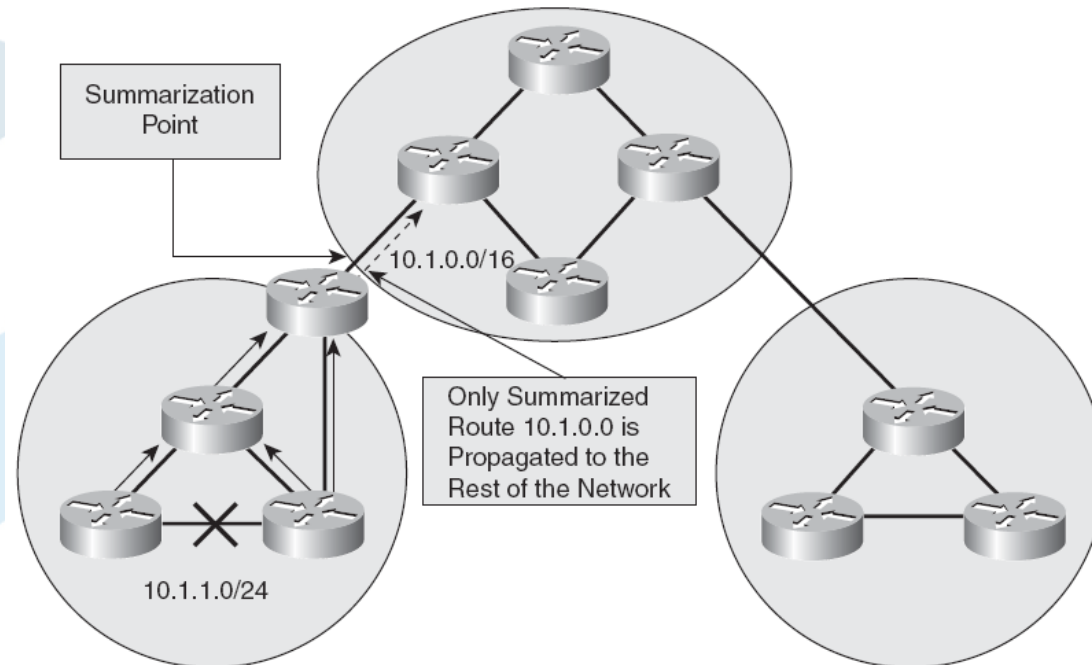
- ✓ Excess routing traffic **consumes bandwidth**
- ✓ Increased routing table **recalculation**
- ✓ Possibility of routing **loops**



Benefits of Route Aggregation

➤ If a link within an area fails, routing updates **are not propagated** to the rest of the network.

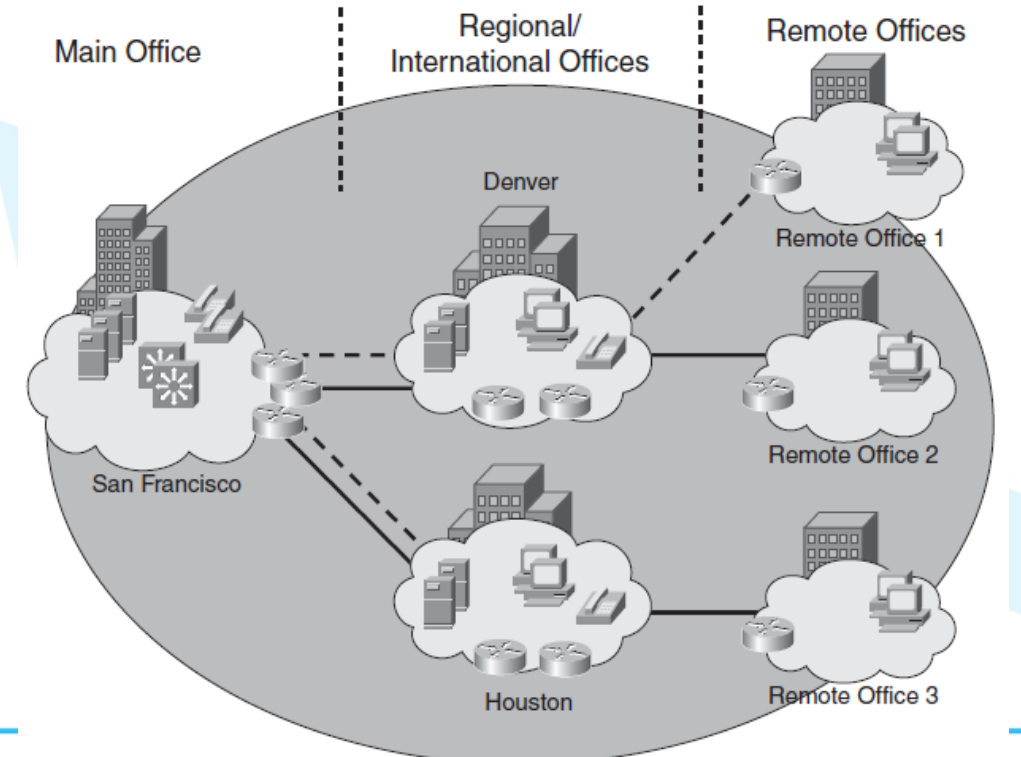
- ✓ Only the **summarized route is sent** to the rest of the network, and it has not changed.
- ✓ The route information about the failed link **stays** within the area.
- ✓ This **reduces bandwidth** consumption related to routing overhead and relieves routers from unnecessary routing table recalculation.



مثال

❖ على فرض البنية الموضحة في الشكل حيث أنه تتوافر لديك المعلومات الموضحة في الجدول

Location	Office Type	Workstations	Servers	IP Phones	Router Interfaces	Switches	Firewall and Other Device Interfaces
San Francisco	Main	600	35	600	17	26	12
Denver	Regional	210	7	210	10	4	0
Houston	Regional	155	5	155	10	4	0
Remote Office 1	Remote	12	1	12	2	1	0
Remote Office 2	Remote	15	1	15	3	1	0
Remote Office 3	Remote	8	1	8	3	1	0
Total		1000	50	1000	45	37	12



مثال

❖ استخدم النطاق التالي من العناوين IP ، 172.16.0.0/16 ، واقترح عنونة مناسبة للمخطط، تستفيد من تقنيات التلخيص بناء على المعلومات المزودة. (أي املأ الجدول التالي بالقيم المناسبة).

Location	Number of IP Addresses Required	Rounded Power of 2	Number of Host Bits ¹	Address Block Assigned
San Francisco				
Denver Region	X			
Denver Campus				
Remote Office 1				
Remote Office 2				
Houston Region	X			
Houston Campus				
Remote Office 3				



الحل

Location	Number of IP Addresses Required	Rounded Power of 2	Number of Host Bits ¹	Address Block Assigned
San Francisco	1290	2048	11	172.16.0.0–172.16.7.255/21
Denver Region	×	1024	10	172.16.8.0–172.16.11.255/22
Denver Campus	441	512	9	172.16.8.0–172.16.9.255/23
Remote Office 1	28	64	6	172.16.10.0/26
Remote Office 2	35	64	6	172.16.10.64/26
Houston Region	×	1024	10	172.16.12.0–172.16.15.255/22
Houston Campus	329	512	9	172.16.12.0–172.16.13.255/23
Remote Office 3	21	64	6	172.16.14.0/26



شكراً لحسن الاستماع هل من أسئلة؟

