شـرح مبسـط لــ

CCNA

تأليف

أحمد عبد الرحمن على شريف

ABOMONA77@YAHOO.COM

00249123842491

00249922346688

شركة ناس طباعة
اسم الكتاب : شرح مبسط لــCCNA
اسم المؤلف : احمد عبد الرحمن على شريف محمد
رقم الايداع :٢٠١٣/٩٩٩٠

رقم الايداع
٢٠١٣/٩٩٩٠

قال تعالى :

(وَيَسْأَلُونَكَ عَنِ الرُّوحِ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُم مِّن الْعِلْمِ إِلاَّ قَلِيلاً)

صدق الله العظيم
سورة الاسراء -٨٥

الإهــــداء

يقف اليراع عاجزاً عن خط كلمات فى حقهم

إلى من وهباني الحياة

أبى وامى

إلى من وهبتني الإحساس الرائع بالأشياء دوماً

إبنتى (منى)

إلى أرواح الشهداء

ابوبكر مجذوب محمد نور
حذيفة فتحي حسن مدني
إلى روح الفقيد منتصر انور
إلى دفعه CTS97

الشكر والعرفان

الشكر لله... ثم

إلى د. ابوبكر إبراهيم

إلى السيد / أسامة خطاب (السفارة السودانية بالقاهرة)

إلى أسرة المهندس / حمدي على محمد على

إلى أسره كلية الهندسة جامعة القاهرة

إلى كل من ساهم في إخراج الكتاب بهذه الصورة

إلى كل من ساندني معنوياً

مقدمة :

يتناول الكتاب فكرة عامه عن CCNA فان اصبنا فهذا فضل من الله وان اخطأنا نرجو منكم مدنا بالمعلومه حتى تعم الفائده وهى تجربة نسال الله لنا التوفيق فيها وان يستفيد منها مستخدمى الحاسوب .

والله من وراء القصد

تعريف الحاسوب :

هــو جهاز اليكترونى يقوم بمعالجة البيانات للحصول على معلومات مفيده

**** المكونات الرئيسة للحاسوب :***

يتكون من مكونين رئيسين هما

١/ المكونات المادية HARD WARE

٢/ البرامج SOFT WARE

(١)المكونات المادية HARD WARE

وهى اى جزء ملموس محسوس فى الحاسوب مثلاً

Key Board ; Mouse ; Moniter ....

(٢) البرامجSOFT WARE

وهى الاوامر التى تقوم بتشغيل الHARD WARE وهى تنقسم الى

١/ برامج تشغيل

٢/ برامج تطبيقية

(١) برامج تشغيل

مثال...........‚ UINX; LINX ; WINDOWS

(٢) برامج تطبيقية

مثال MOICROSOFT OFFICE;VISUALBASIC ; AUTO CAD

**** وهنالك عده انواع من الحاسبات :-***

١/ اجهزة الكمبيوتر الطرفية INTELLIGET TERMNAL

وهى اجهزه متكاملة تحتوى بداخلها على وحده معالجة مركزية يتم استدعاء البيانات من اجهزة الكمبويتر Main Frame

2/ تجهزة الكمبيوتر الطرفية محدودة القدرة DUMB TERMINALS

وهى تستخدم لادخال البيانات وعرضها فحسب

٣/ اجهزة الكمبيوتر الصغيرة MINI COMPUTER

وهى ذات قدرات تم تصميمها كتطوير للاجهزة الكبيرة

٤/ اجهزة الكمبيوتر الفائقة SUPER COMPUTER

لها قدرات عاليه فى معالجة البيانات وهى تستخدم فى مراكز الابحاث والمؤسسات العسكرية .

٥/ اجهزة الكمبيوتر الشخصية PERSONAL COMPUTER

وهى المستخدمة حاليا فى المكاتب والمؤسسات والمنازل

٦/ اجهزة المحمول PRATABLE COMPUTER

LAP TOP وهى تطوير لاجهزة ال PC

***وينقسم الحاسوب الى ثلاث وحدات :-**

١/ وحدة الادخال IN PUT Units

٢/ وحدة المعالجة المركزية CPU

٣/ وحدات الاخراج OUT PUT Units

***(١)وحدات الادخال** IN PUT Units

ومهمتها ادخال البيانات الى جهاز الحاسوب عبر وحدات الادخال المختلفة ومنها

***١/ لوحة المفاتيح** KEY BOARD

تقوم بادخال الحروف من أ... ى & Z.....A& والارقام من ٠........٩ & والرموز -.+ }.{./.*.>.< ....الخ

***٢/ الفاره** MOUSE

يسمح بالتنقل بين البيانات والخيارات المتاحة

***٣/ القلم الضوئي** LIGHT PEN

يستخدم فى الاشارة الى الاجزاء المختلفة من الشاشة واختيار الاوامر

***٤/ عصا الالعاب** JOY STIC

تستخدم فى التوجية والتحريك

***٥/ الماسح الضوئي**SCANNER

يستخدم لادخال الصور والاشكال

***٦/ الميكرفون**MICROPHONE

يستخدم لادخال الصوت الى الحاسب

***٧/الكاميرا** CAMERA

يمكن استخدامWEB CAM لادخال الفيديو والصور الى الحاسوب

***(٢) وحده المعالجة المركزية** CPU

وتنقسم الى ثلاث وحدات

1/ C.U
2/ A.L.U
3/MEM

***١/ وحدة التحكم** C .U

تقوم بنقل البيانات من وحدات الادخال الى وحده المعالجة المركزية لتتم معالجتها ومن ثم نقلها الى وحدات الاخراج

***٢/ وحدة الحساب والمنطق**A.L.U

وهى الوحدة المختصة بالعمليات الحسابية والمنطقية

***٣/ وحدة الذاكرة** MEM

وهى تقوم بحفظ البيانات بعد ان تتم معالجتها

(٣) وحدات الاخراج OUT PUT Units

وهى تقوم باخراج البيانات بعد ان تتم معالجتها بالصورة المطلوبة وهنالك عده انواع من وحدات الاخراج

١/ الشاشة MONITOR

وتستخدم لاستخراج المعلومات وعرض الصور والنصوص

٢/ الطابعة PRINTER

تستخدم لاستخراج المعلومات مطبوعة على ورق

٣/ السماعة SPEAKER

وتستخدم لاستخراج الصوت

٤/ اجهزة العروض التقديمية PROJECT DIVICE

ويمكن توصيلها بالحاسوب للعروض التقديمية

تعريف شبكات الحاسوب:(Computer Network)

الشبكة هي عبارة عن جهازين او اكثر متصلة مع بعضها البعض عن طريق وسائط الاتصال الخاصة بكروت الشبكة مثل (كروت الشبكة ، الاسلاك ، نقاط الاتصال ، وغيرها

استخدامات الشبكة:(Network Using)

يمكن تصنيف الاستخدامات الى قسمين:

استخدام خاص بالشركات:(Companies Network)

في بعض المؤسسات الكبيرة نجد عدد هائل من اجهزة الحاسوب ولسهولة عملية التداول والتبادل في الملفات والمشاركة في الخدمات التي تتيحها الشبكات ولتوفير تلك الخدمات لابد من تصميم شبكة داخلية تلائم هذا العدد الهائل من اجهزة الحاسوب ولعل الفائدة للشركة جراء تلك الشبكة تقتصر في الاتي:

مشاركة الادارات المختلفة في الملفات:(File Sharing)

حيث تتيح الشبكة للشركة خدمة تبادل الملفات عن طريق برتكول تبادل الملفات او برتكول نقل الملفات (FTP) وهو اختصار الـــــــــــــ.(File Transfer Protocol)

مشاركة الطباعة:(Printing Sharing)

يمكن ربط الطابعة شبكيا وهناك طابعة تسمى بالطابعة الشبكية والتي لا تتصل بالملقم مباشرة ولكنها تكون عقدة (Node) مثل كل العقد الموجودة في الشبكة ويكون لها كرت شبكة وعنوان IP خاص بها وهي تجعل مشاركة الطباعة شبكيا عملية سهل جدا بين الادارات المختلفة في المنشأة.

حفظ الزمن وتوفيرا للمال.(Save Time & Money)

مشاركة خدمة الاتصال بالانترانت والانترنت (Internet & Intranet Sharing Service)

يمكن من خلال الشبكة مشاركة خدمة الاتصال بالانترانت لتبادل الخطابات والمذكرات الداخلية و خدمة البريد الالكتروني داخل المنشأة ويمكن مشاركة الاتصال بخدمة الاتصال بالانترنت وتصفح المواقع.

استخدام خاص بالافراد:(Personnel Network)

وهي لا تختلف عن الشبكة الخاصة بالشركات ولكن الاختلاف يكون في كمية اجهزة الحاسوب المتصلة مع بعضها البعض اما الشبكة الخاصة بالافراد فيمكن توصيل عدد (٣) جهاز حاسوب بالشبكة ومشاركة جميع الخدمات التي تتميز بها شبكة الشركات والتي اقتصرت في الاتي:

مشاركة الطباعة على الشبكة(Printing Sharing)

مشاركة الاتصال بخدمة الانترانت والانترنت

(Internet & Intranet Sharing Service)

لتبادل ونقل الملفات على الشبكة(File Sharing)

شبكات ويندوز٢٠٠٠:(Windows 2000 Network).

صمم هذا النظام ليكون النظام الخاص بالشبكات بعد ويندوز NT.4 وهو نظام كبير وعتيق ومتطور لدرجة كبيرة ويمكن من خلاله تصميم وادارة شبكة كبيرة وصغيرة على حد سواء ويدعم كل الخدمات الشبكية المعروفة وقد تم اصدار ثلاثة انواع من الملقمات في ويندوز ٢٠٠٠ وهي:

ويندوزسيرفر٢٠٠٠:(Windows 2000 Server)

وهو يعتبر المثالي للشبكات الصغيرة والمتوسطة الحجم لنشر الملقمات الخاصة بالملفات والبرامج والطباعة والاتصالات ويدعم عدد ٤ معالجات و ٤ غيغابايت من الذكرة المادية.

ويندوزسيرفر المتقدم:(Windows Advanced Server)

فيه كل مميزات ويندوز ٢٠٠٠ ويزيد بدعمه لعدد ٨ معالجات وامكانية الاستفادة من الذاكرة فهو مثالي لقواعد البيانات والاعمال المكثفة.

ويندوز 2000 ***مركز البيانات***:(Data Center)

وهو ملقم مركز البيانات وهو مخصص للشبكات الكبيرة الخاصة بالشركات الضخمة وهو مثالي لمزود خدمات الانترنت (ISP) وهو اختصار
لـــــــ (Internet Service Provider) وهو يدعم حتى ٣٢ معالج.

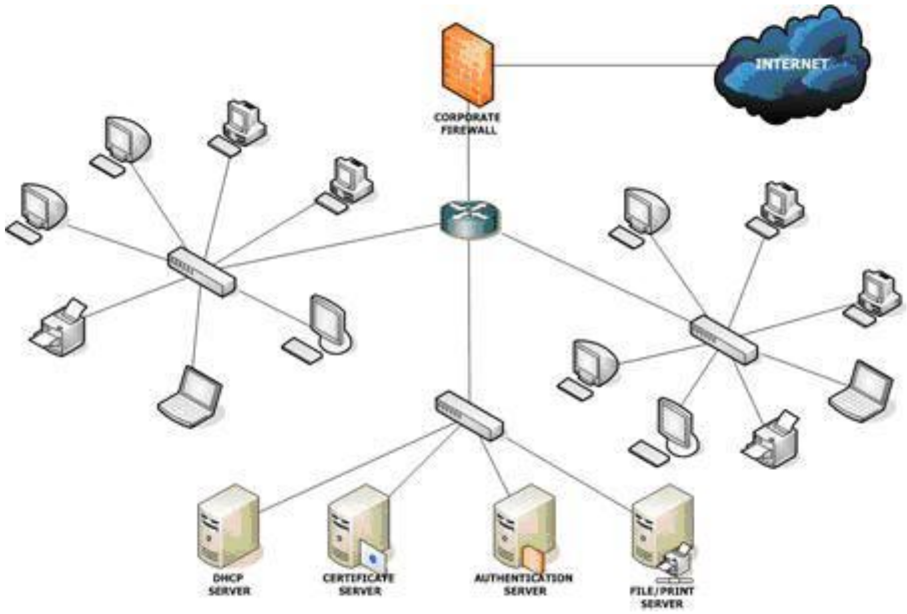
انواع الشبكات: (Network Type)

الشبكة المحلية.(Local Area Network).................................. (LAN)

شبكات المدن.(Metropolitan Area Network)........................(MAN)

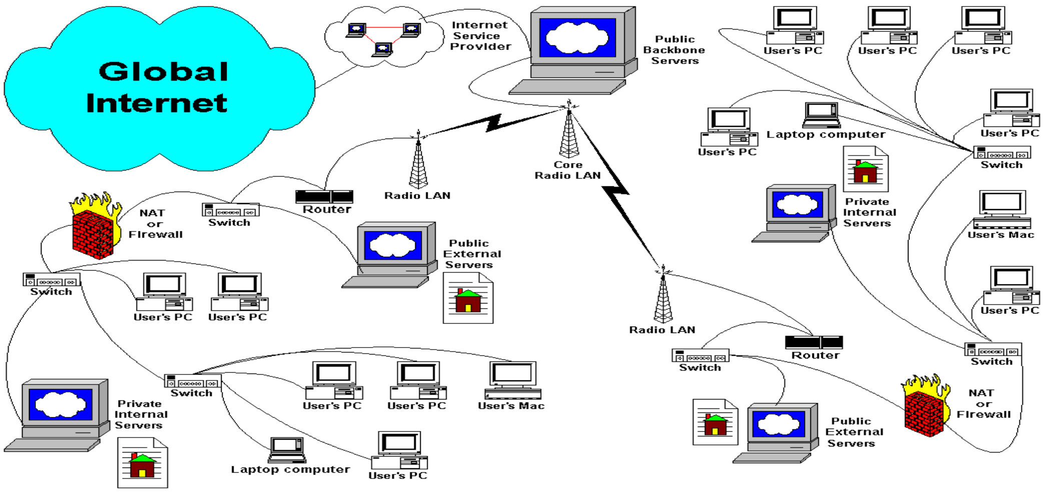
الشبكات الواسعة النطاق.(Wide Area Network)....................... (WAN)

(١) الشبكات المحلية:(LAN)



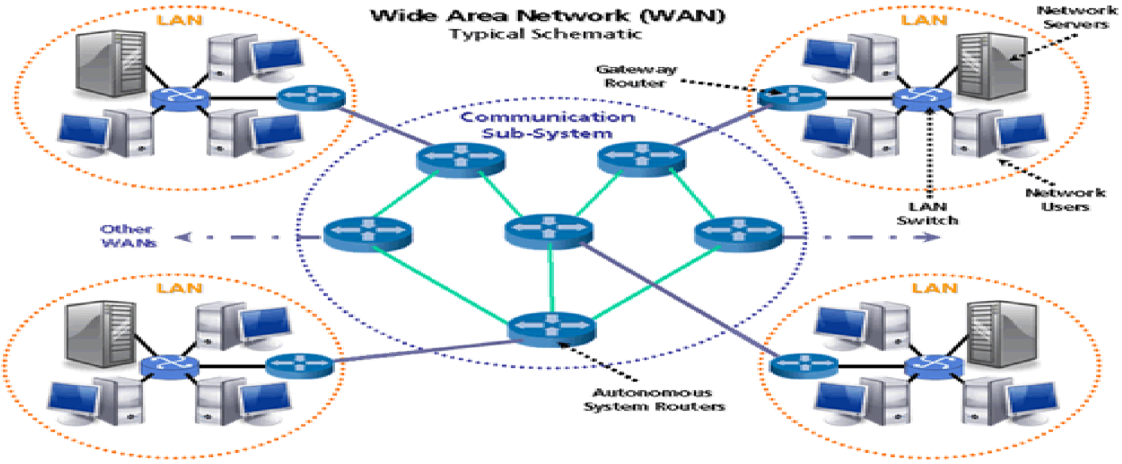
وهي شبكة محلية يتم تركيبها في مبنى واحد أو مبنيان ذات مسافة قريبة جدا وهي تستخدم لربط أجهزة الحاسوب في الإدارات المختلفة داخل المنشأة هذا بالنسبة للمؤسسات أو الشركات أما بالنسبة للإفراد فيمكن توصيل شبكة محلية منزلية تربط جهازين أو أكثر.

(٢) *شبكات المدن*:(MAN)



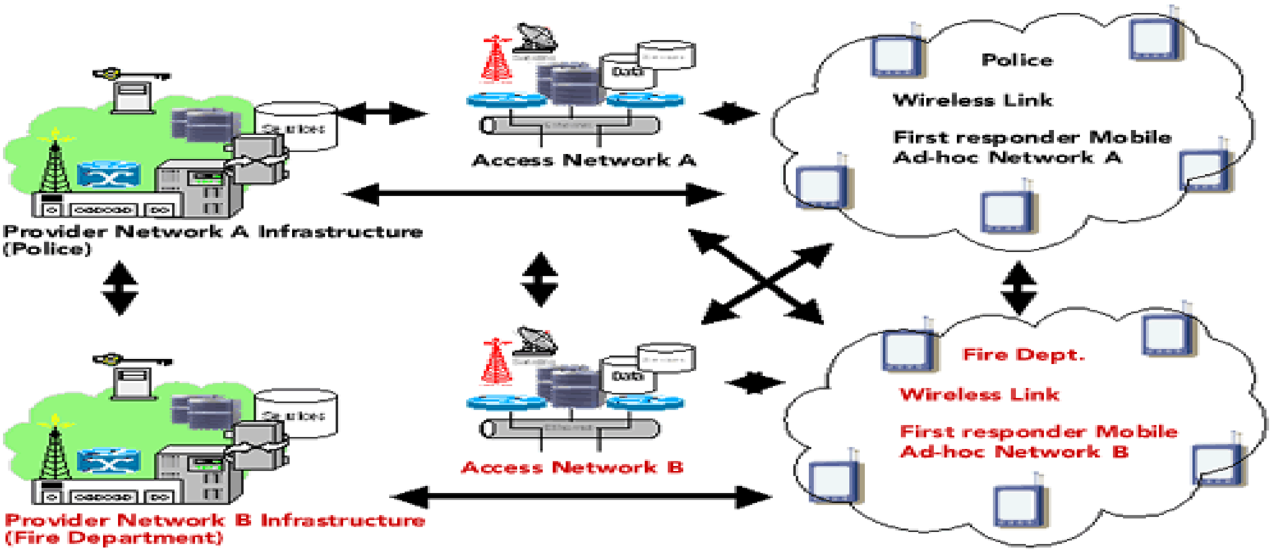
هي شبكة قيل عنها إنها من تصنيف الشبكات المحلية وهي شبكة خاصة بربط المدن مع بعضها البعض عن طريق الألياف الضوئية (Fiber Optic) أو الشبكة اللاسلكية (Wireless Network)مثلا شبكة تربط بين مدينتي الخرطوم – مدني حيث تستخدم الألياف البصرية.

(٣) *الشبكة الواسعة النطاق*:(WAN)



وهي شبكة واسعة النطاق ذات أبعاد جغرافية هائلة وهي تربط بين الدول عبر ما يسمي بالكابلات البحرية مثلا ما يربط دولتي السودان – المملكة العربية السعودية الكابل البحري الذي يمر بالبحر الأحمر.

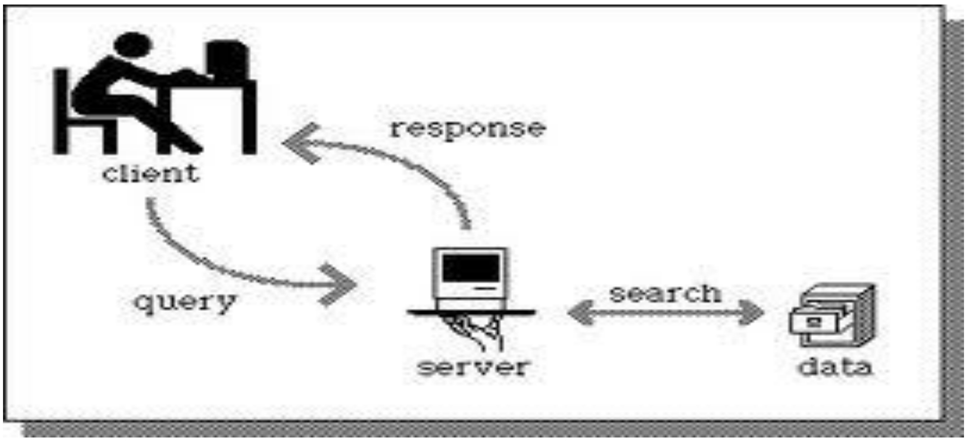
٤/ الشبكة العالمية:(Internet)



الشبكة العالمية هي الانترنت حيث يتم الاتصال به عبر أجهزة الستالايت (Satellite) و كابلات (Coaxial Cable) والانترنت هي (World Wide Web) أو (WWW) أو ما يسمى بالشبكة العنكبوتية وهي تتكون من خدمات معلوماتية واسعة تسمح للمستخدمين لتصفح المعلومات.

(٥) تصنيفات الشبكات : (Network Classifications)

(أ) شبكة الزبون / الخادم:(Client / Server)



يعرف هذا النوع من الشبكات بالشبكات ذات المخدم تستخدم أحد حواسيبها لحفظ المعطيات ذات الإستخدام الجماعي، وتلبية طلبات الخدمة الواردة من محطات العمل.

محاسن شبكات المخدم والزبون. أ:

*تؤمن سرعة كبيرة في معالجة المعطيات.

*تملك نظام حماية آمن للمعلومات وتؤمن السرية كذلك.

*سهولة في التحكم إذا ما قورنت بالشبكات المتكافئة.

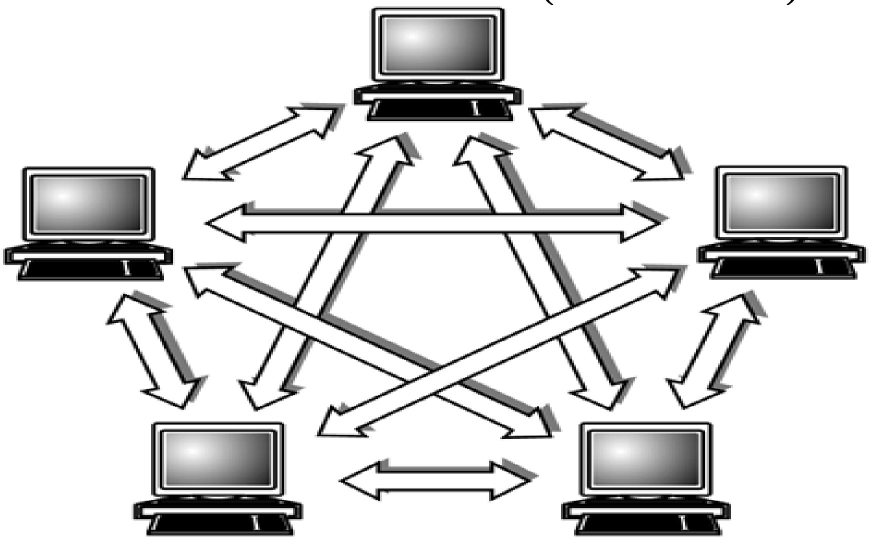
عيوب شبكات المخدم والزبون.:ب

*تتطلب هذه الشبكات تخصيص حاسوب لإستخدامه كمخدم وبالتالي فإن هذه الشبكات تكون عادة أغلى سعراً.

*تتعلق سرعة أداء الشبكة ووثوقيتها بالمخدم المستخدم.

*هذه الشبكات أقل مرونة بالمقارنة مع الشبكات المتكافئة.

(ب) شبكة الند للند (Peer To Peer)



الشبكات المتكافئة هي الشبكات التي لا يكون فيها مركز واحد للتحكم بالعلاقة بين محطات العمل ، وليس فيها جهاز واحد لحفظ المعطيات ، يكون نظام التشغيل في هذه الشبكة موزع على كافة محطات العمل ، لذلك فإن كل محطة عمل تكون قادرة على تنفيذ مهام المخدم في تلبية الطلبات الواردة من محطات أخرى إضافة إلى وظائف المستخدم التي تمثله، أي ترسل طلبات إلى محطات عمل أخرى ، وهذا كله بآن واحد معاً ، كافة الأجهزة المتصلة بكافة محطات العمل من طابعات وأقراص صلبة وسواقات أقراص ليزرية وغيرها ، تكون متاحة بشكل كامل لكل مستثمر في الشبكة في حالة الحصول على سماحية مدير الشبكة.

أ. محاسن الشبكات المتكافئة:

*كلفة هذه الشبكات قليلة ، إذ أنها تستخدم كافة الحواسيب المتصلة بالشبكة كمحطات عمل.

*وثوقيتها عالية ، إذ في حال تعطلت إحدى محطات العمل ، يتعزر الوصول إلى بعض المعطيات التي تحويها الشبكة وليس كلها.

ب. سلبيات الشبكات المتكافئة:

*الإرتباط الوثيق بين فعالية الشبكة وعدد المحطات التي تعمل بآن واحد في نفس اللحظة.

*صعوبة تنظيم التحكم الفعال بين المحطات.

Router

يقوم جهاز الراوتر بإرسال وتوجيه الحزم الإليكترونية Packets إلى اجهزة الاستقبال وتعد مهمته الأساسية هي تحديد الطريق السليم الذي ستعبر منه هذه الحزم لجهة المستقبل,

يحتوي جهاز الرواتور على سوفت وير مخصص لهذه العملية بجانب مزايا وخدمات اخرى سنتعرف عليها بعض قليل، من كبرى الشركات في تصنيع اجزة الراوتر هي شركات Cisco و Juniper ولدارسين شهادات هذه الشركات هذه السوفت وير لها اسماء مثل IOS و JUNOS

يقع لدى عدة مستخدمين لبث شديد عندنا يطلقون على اجهزة الـــ ADSL Modems والتي يؤجرونها من شركات تزويد خدمة الانترنت او يشتروها – يطلقون عليها راوتر وهذا خاطيء تماماً فهذه الاجهزة ليست سوى Modem يقوم بعملية تحويل البيانات من رقمية إلى تناظرية Digital to Analogue ولكن هذه الاجهزة لا تقوم بوظيفة الرواتر الاساسية وهي توجيه الحزم إلى المسارات الصحيحة...

***وظيفة الموجه* Router ؟**

يقوم الراوتر بتوصيل شبكتين او اكثر غير متقاربتين او متقاربتين (مثل على ذلك شبكة في الخليج وشبكة في السودان) مع بعضهم البعض وذلك من خلال معرفة المسار الذي يؤدي إلى الراوتر الاخر وذلك من خلال عدة موجهات اخرى!

***يوجد نوعان من الموجهات*:**

١/ موجه يعرف ويحدد المسارات التي سوف يتخذها للوصول للطرف الأخر.

٢/موجه يقوم بإرسال الحزم إلى المسار القادم مباشرة بدون تحديد مسار أفضل

ولكن ماهي المسارات وكيف يوجد مسار افضل من الاخر وكيف يحددها الراوتر؟؟ بالطبع هناك مسارات افضل من الاخرى (اي اقصر او توفر وقتاً) فإذا قلنا ان هناك بيننا وبين دولة الدول الاوربية ٥٠ راوتر كلاً واصلين تلو الاخر (وهذا ما يحدث في الحقيقة) كلاً من هذه الموجهات موجود في مدن عدة منها اقرب ومنها ابعد -يقوم الراوتر لدينا بالتحدث مع الراوتر الذي يليه وبالتالي يرسل للذي يليه وهكذا حتى يحدد اقرب طريق (وهذه طريقة واحدة من عدة طرق) وبهذا يحدد اي مسار افضل واذا كان هناك مسار مشغول يمكن ان يتجنبه عن طريق مسار اخر.

***يوجد عدة انواع من الموجهات من حيث الخدمة والحجم*:**

بالطبع اجهزة ADSL Modem والتي نراها في منازلنا لا يتعدى حجمها حجم كتاب كبير – ولكن هل تعلم ان هناك موجهات يتعدى حجمها الثلاجة؟

***١/ موجهات للإستخدام المنزلي والإستخدام الداخلي*:**

تعمل هذه الموجهات على نطاق صغير بمعنى انها تخدم وسائل الانترنت وتحديد المسارات القادمة ولكنها بعد ان ترسل الحزمة لا تقوم بالإحتفاظ بالمسار الذي استخدمته.

ايضاً من عيوب هذه الموجهات ان في بعض الاحيان تصلها حزم كبيرة لا تستطيع تحويلها كاملة وبالتالي تفقد هذه الحزم.

٢/ موجهات تستخدم للمكاتب الصغيرة:

يتم إطلاق لقب Gateway عليها وهي تعني المعبر – وتقوم بإيصالك بشكبات اكبر منها مثل الانترنت ومن مميزاتها انها تجعل عدة اجهزة كمبيوتر تعمل عليها بأن تظهر كجهاز واحد فقط على شبكة الانترنتResidental Gatewar

٣/ موجهات تستخدم على نطاق المؤسسات الكبرى:

يكون حجم هذه الاجهزة ضخم ويمكن وجودها في الجامعات ومراكز تزويد خدمة الانترنت ISPsتعتبر من افضل الموجهات نظراً للخدمات العدة التي تقوم بها ويطلق عليها دائما مصطلح Level 3 Model ماهو الموجهRouter ؟

يقوم جهاز الراوتر بإرسال وتوجيه الحزم الإليكترونية Packets إلى اجهزة الاستقبال وتعد مهمته الأساسية هي تحديد الطريق السليم الذي ستعبر منه هذه الحزم لجهة المستقبل,

يحتوي جهاز الرواتور على سوفت وير مخصص لهذه العملية بجانب مزايا وخدمات اخرى سنتعرف عليها بعض قليل، من كبرى الشركات في تصنيع اجزة الراوتر هي شركات Ciscoو Juniper ولدارسين شهادات هذه الشركات هذه السوفت وير لها اسماء مثل IOS وJUNOS

يقع لدى عدة مستخدمين لبث شديد عندنا يطلقون على اجهزة الـــ ADSL Modems والتي يؤجرونها من شركات تزويد خدمة الانترنت او يشتروها – يطلقون عليها راوتر وهذا خاطيء تماماً فهذه الاجهزة ليست سوى Modem يقوم بعملية تحويل البيانات من رقمية إلى تناظرية Digital to Analogue ولكن هذه الاجهزة لا تقوم بوظيفة الرواتر الاساسية وهي توجيه الحزم إلى المسارات الصحيحة...

Switch

هو عبارة عن جهاز متعدد البورتات مثل الHUB عند تشغيله يقوم بفحص الفريمات التي تأتيه من كل جهاز متصل باي بورت من بورتاته ويأخذ ال Source MAC ويضعه في جدول كل Mac وما يقابله من ,,, Port عند الانتهاء من هذه العملية يكون لديه جدول بكل الأجهزة المتصله به وعلى أي منفذ هي متصلة وهذه المرحلة تسمى Learning وفيها لا يقوم السويش باتخاذ اي قرار ولا يمرر اي فريم عندما يريد اي جهاز متصل بالسويتش ارسال اي فريم لجهاز آخر ، يقوم السويتش بقراءة الفريم ومعرفة وجهة الفريم destination MAC addressويقارنها مع الجدول,,,, MAC address table ان كان عنوان الوجهة موجودا في الجدول : يقوم بارسال الفريم الى البورت المحدد في الجدول ويسمى هذا Forwarding وهنا تكون حركة البيانات بين هذين المنفذين على شكل قناة ان كان عنوان الوجهة غير موجود في الجدول : يقوم السويتش بتجاهل الفريم وحذفه Filtering حركة الفريمات بين كل جهازين تكون في قناة منفصلة لا يحدث فيها تداخل مع الأجهزة او المنافذ الأخرى ، خلافا لل HUB الذي يقوم بارسال الفريم الذي يأتيه من منفذ الى كل المنافذ ويتسبب هذا في اهدار حزمة البيانات Bandwidth وحدوث كثير من التصادمالى هنا يتم التعامل مع الفريمات التي تأتي من جهاز معين الى جهاز معين وتسمىUnicast اجهزة الشبكة قد تحتاج الى ارسال فريمات او بيانات الى كل الأجهزة Broadcastونعرف ان لكل كرت شبكة MAC Address فريد ما الحل؟ يتم استخدام FFFF.FFFF.FFFF وهو Mac Address يتم عن طريقة ارسال الفريمات لكل الاجهزة وكل حزمة يكون destination MAC address يتم اعتراضها من كل جهاز على انها مرسلة له ولذلك يقوم السويتش بارسال الفريمات الى كافة منافذه Multicast addressesفي هذه الحالة هناك اجهزة او برامج ذات طبيعة واحدة وقد تستخدم برتوكول معين وهي مهتمة باستقبال Multicast على عنوان معين ،،، هي فقط التي تقوم باعتراض الفريم كانه موجه لها

الفرق بين SWITCH **و** ROUTER

Router

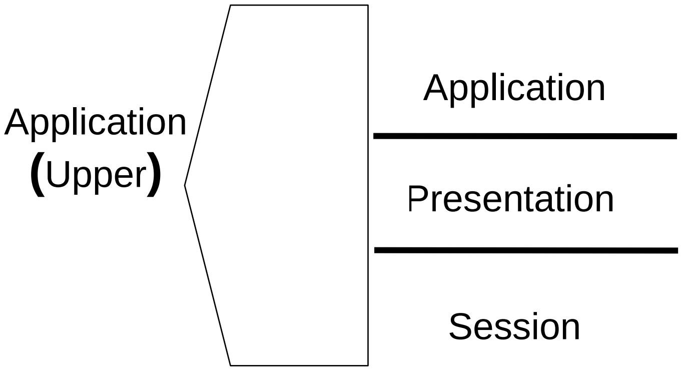
ال Router وظيفته الرئيسية هي عبارة عن ربط مجموعة من الشبكات مع بعضها البعض وفي العادة فانه يتعامل بين الاجهزة عن طريق IP ويقوم الراوتر بربط شبكات ليست في نفس المكان يمكن ان تكون بينهم مسافات بعيدة ومتال على ذلك هو ربط شبكات مزود الانترنت ISP وشبكة محلية LAN وشبكة اخرى WAN

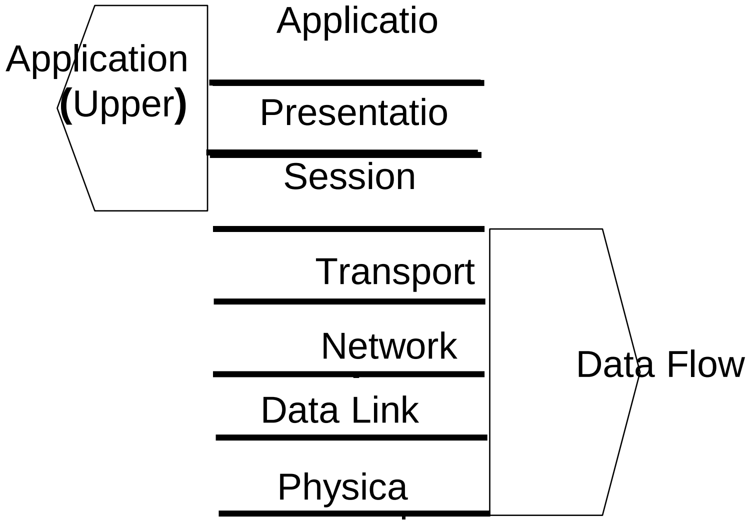
SWITCH

هو عبارة عن جهاز يقوم بربط اجهزة الشبكة مع بعض ويقوم بالتعامل مع هذه الاجهزة عن طريق MAC address ويتميز عن ال bridge انه يحتوي على اكثر من منفذ Port تتراوح بين ٤ و ٦ و٨ و ١٦و ٣٢ ومن ميزاته انه لديه القدرة على التعرف على كل جهاز واي منفذ متصل به هذا الجهاز وفي حال ارسال اي بينات او اشارة من جهاز الى اخر فان هذه البيانات او الاشارة لا تذهب كما هو الحال في ال Hub جميع الاجهزة بل تذهب الى الجهاز المقصود فقط في هذه الحالة فان عملية ال bandwidth تكون شبه معدومة. يمكن ان نقول انه ال switch قد جمع بين ميزات HUB و Bridge وقد تخلى عن عيوبهما

OSI Model Overview

OSI Model Overview



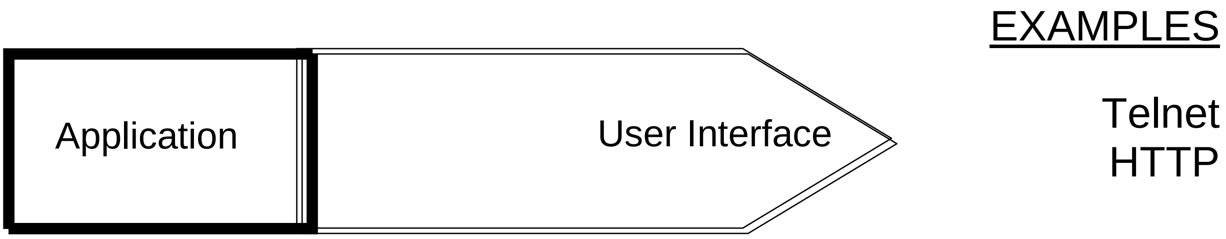


The Data Link layer of the OSI reference model is implemented by Switches and Bridges. These devices encapsulate date in "frames."

The Network layer of the OSI reference model is implemented by Routers. These devices encapsulate data in 'packets.'

The Transport layer of the OSI reference model is implemented by various protocols; one of which is TCP. TCP uses ports and encapsulates the data in 'segments.

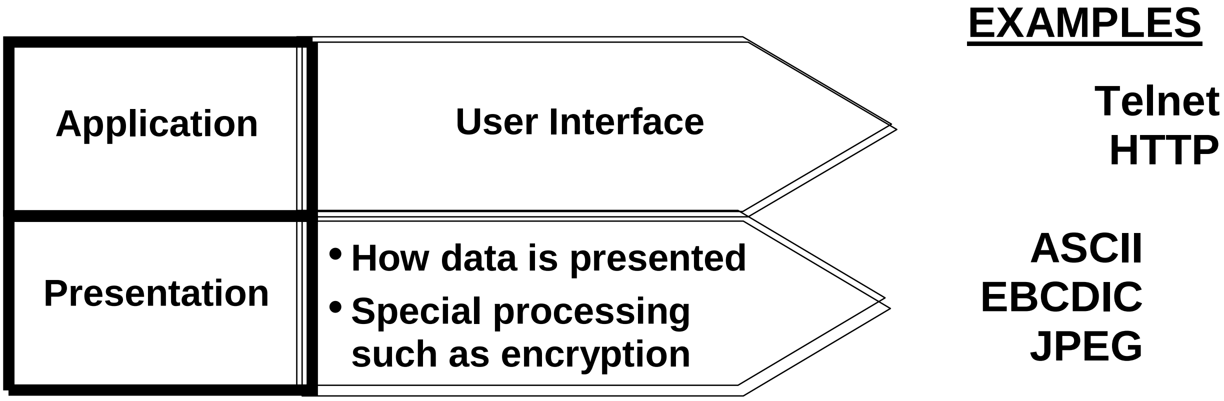
Role of Application Layers



This layer discusses network applications rather than computer applications. So, applications such as spreadsheets, word processors, or presentation graphics are not the applications being described here. Network applications may be applications that support, electronic mail, file transfer, remote access, network management, and so on .

Transition: The following discusses the presentation layer.

Role of Application Layers



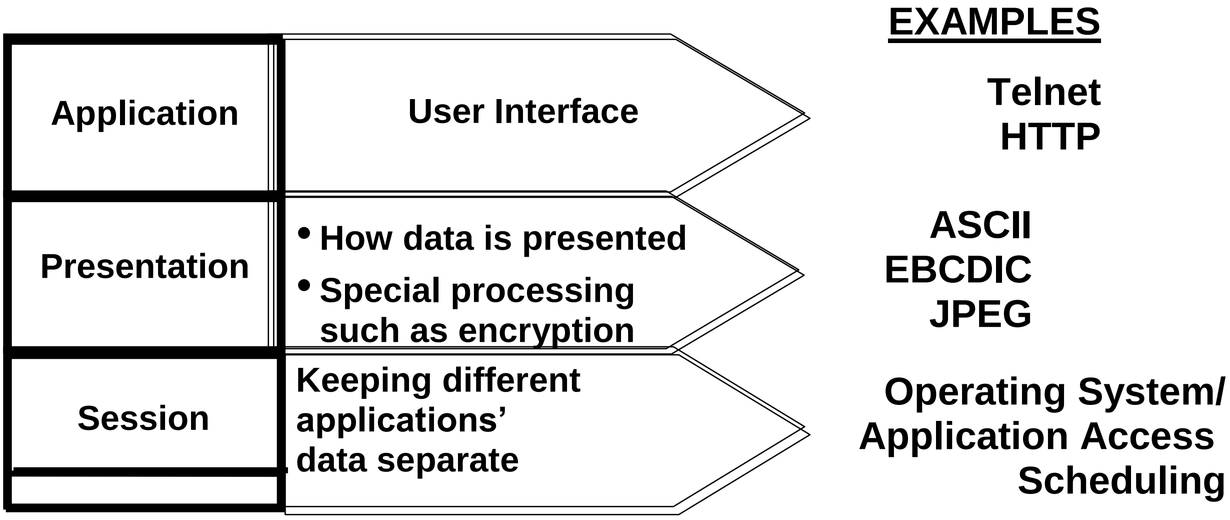
EXAMPLES

Application — User Interface — Telnet HTTP

Presentation — • How data is presented • Special processing such as encryption — ASCII EBCDIC JPEG

This layer discusses code formatting, data presentation standards, and conversion.
Transition: The following discusses the session layer

Role of Application Layers



EXAMPLES

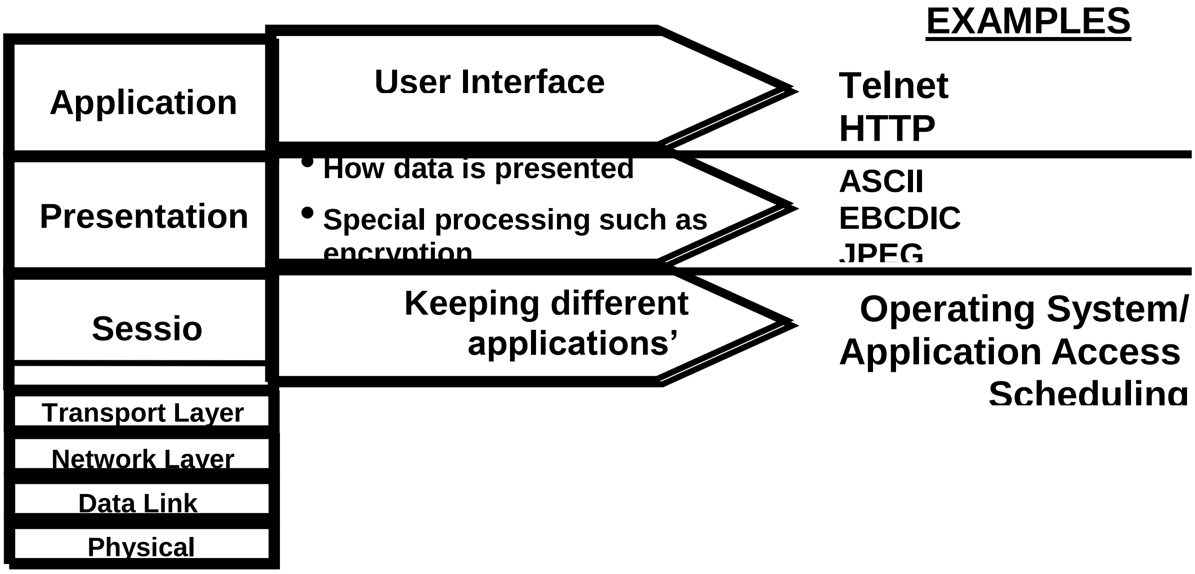
Application — User Interface — Telnet HTTP

Presentation — • How data is presented • Special processing such as encryption — ASCII EBCDIC JPEG

Session — Keeping different applications' data separate — Operating System/ Application Access Scheduling

This layer coordinates applications as they interact on different hosts. Examples of session-layer protocols include: NFS, SQL, RPC, and so on.

.



EXAMPLES

Application — User Interface — Telnet HTTP

Presentation — • How data is presented • Special processing such as encryption — ASCII EBCDIC JPEG

Sessio — Keeping different applications' — Operating System/ Application Access Scheduling

Transport Layer

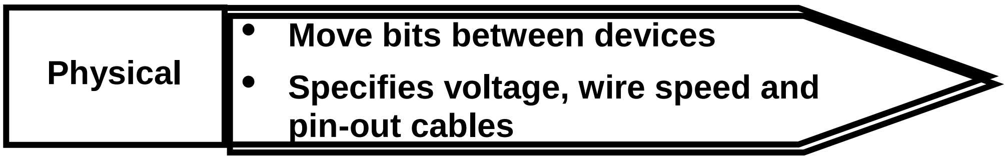
Network Layer

Data Link

Physical

The lower layers sit below the upper three layers. The remainder of this course is focused on the lower layers.

Role of Data Flow Layers



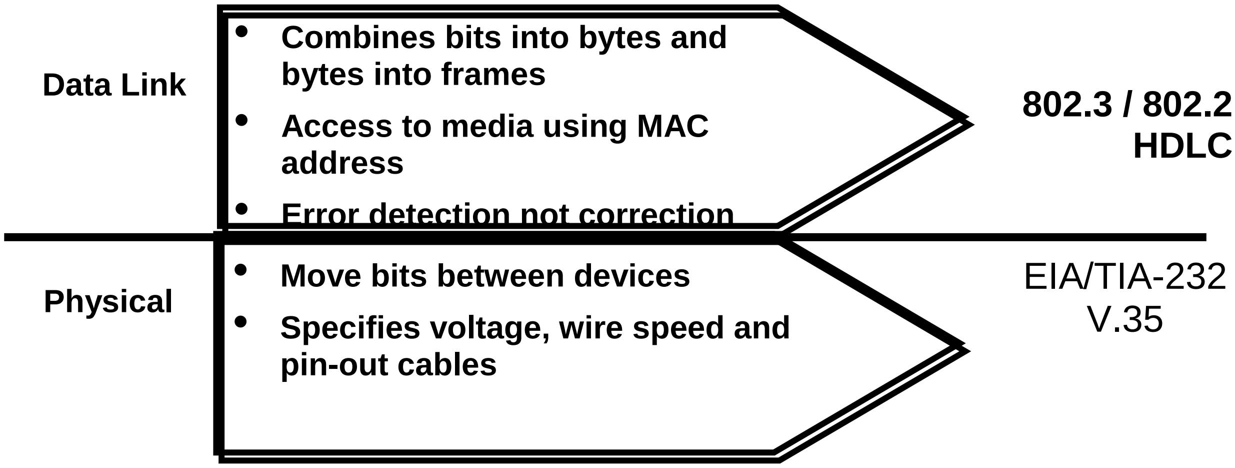
Physical

- Move bits between devices
- Specifies voltage, wire speed and pin-out cables

The physical layer specifies the electrical, mechanical procedural, and functional requirements for activating, maintaining, and deactivating the physical link between systems.

Certain physical standards are associated with certain data link standards. For example, 802.3 is used with data link standard 802.2 for Ethernet. It is not used in WAN connections. This is covered more in-depth later in the course.

Role of Data Flow Layers



Data Link

- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection not correction

802.3 / 802.2
HDLC

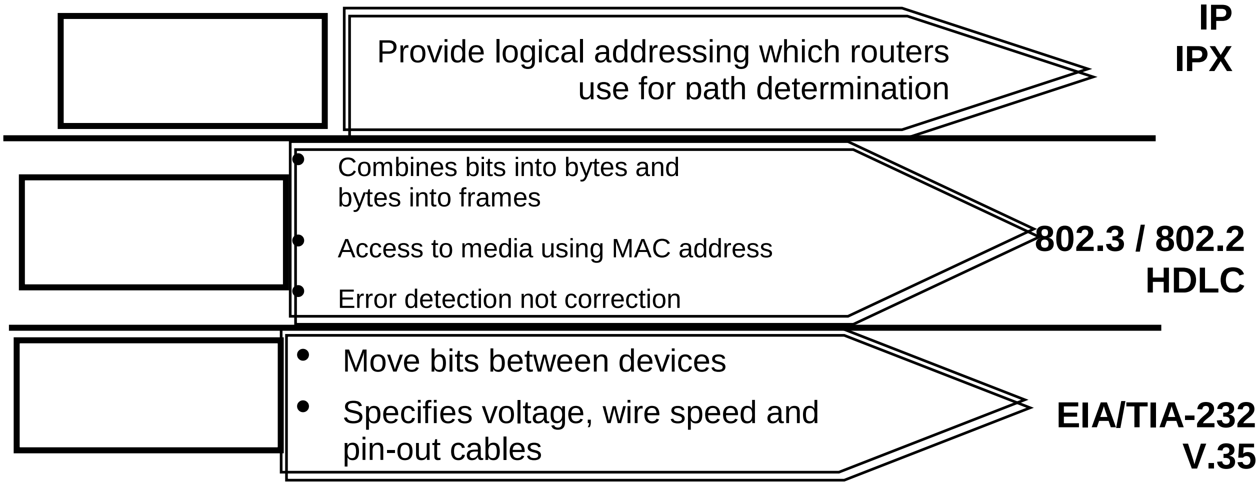
Physical

- Move bits between devices
- Specifies voltage, wire speed and pin-out cables

EIA/TIA-232
V.35

The data link layer provides data transport across a physical link. 802.3 is and physical and data link Ethernet protocol. It is used with the 802.2 standard.

Role of Data Flow Layers



Provide logical addressing which routers use for path determination

IP
IPX

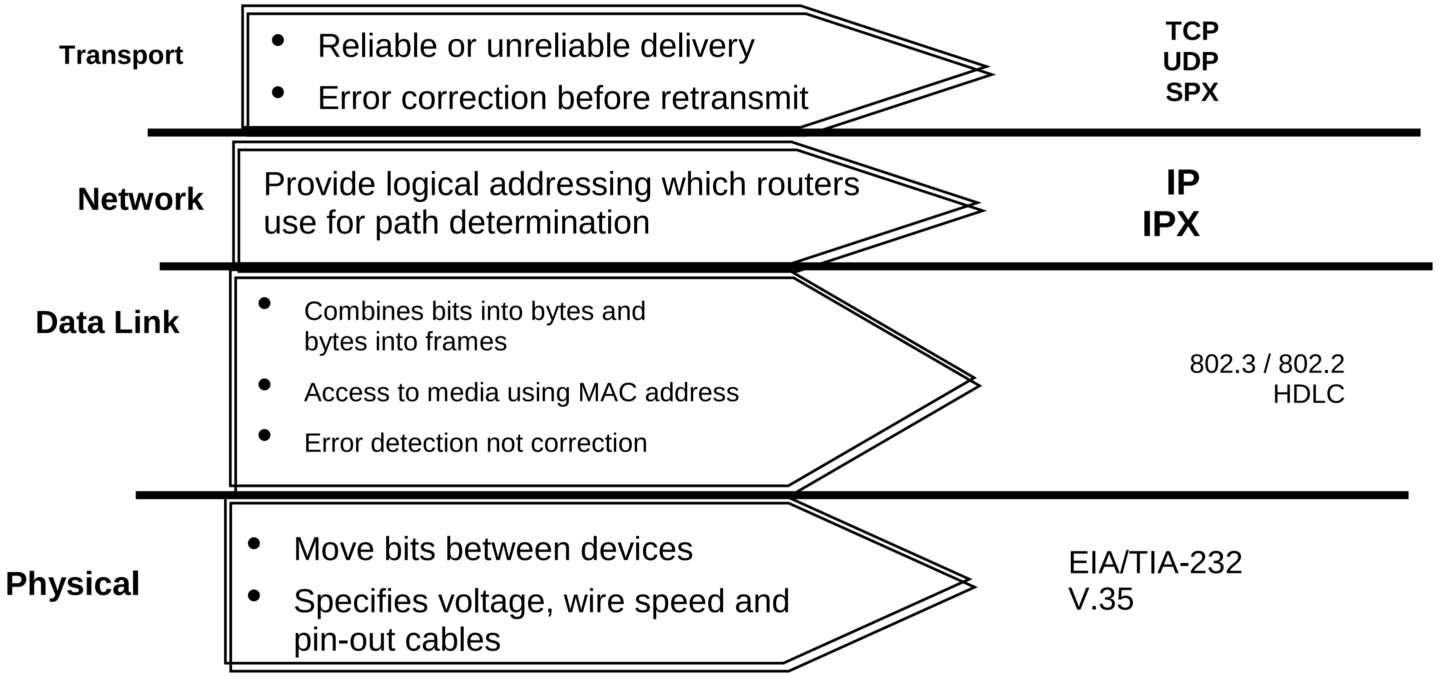
- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection not correction

802.3 / 802.2
HDLC

- Move bits between devices
- Specifies voltage, wire speed and pin-out cables

EIA/TIA-232
V.35

Role of Data Flow Layers



Transport

- Reliable or unreliable delivery
- Error correction before retransmit

TCP
UDP
SPX

Network

Provide logical addressing which routers use for path determination

IP
IPX

Data Link

- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection not correction

802.3 / 802.2
HDLC

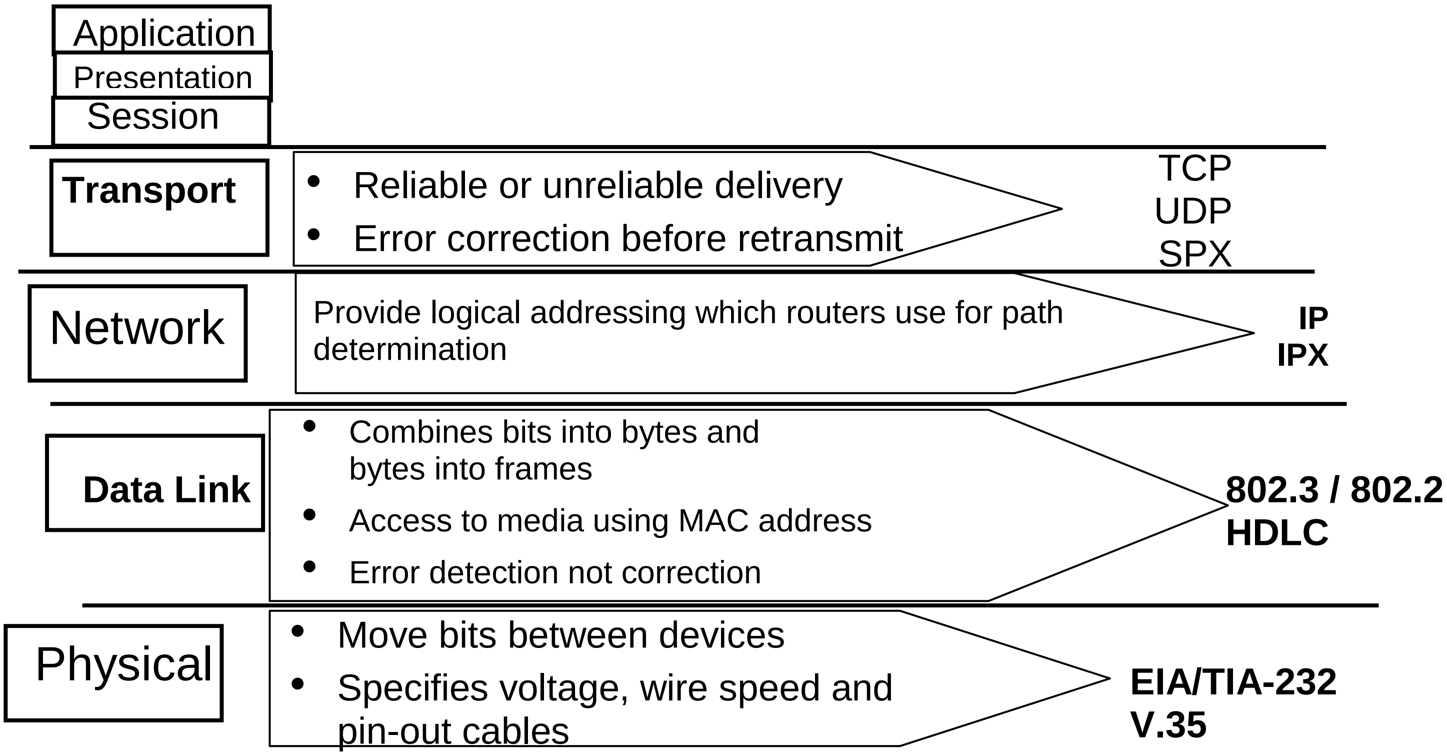
Physical

- Move bits between devices
- Specifies voltage, wire speed and pin-out cables

EIA/TIA-232
V.35

The Transport layer of the OSI reference model is implemented by various protocols; one of which is TCP. TCP uses ports and encapsulates the data in ‘segments’. TCP is connection oriented so it offers reliable service. The other major transport layer protocol discussed in this course is UDP. It offers speed but no reliability because it is connectionless.

Role of Data Flow Layers



Application
Presentation
Session

Transport

- Reliable or unreliable delivery
- Error correction before retransmit

TCP
UDP
SPX

Network

Provide logical addressing which routers use for path determination

IP
IPX

Data Link

- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection not correction

802.3 / 802.2
HDLC

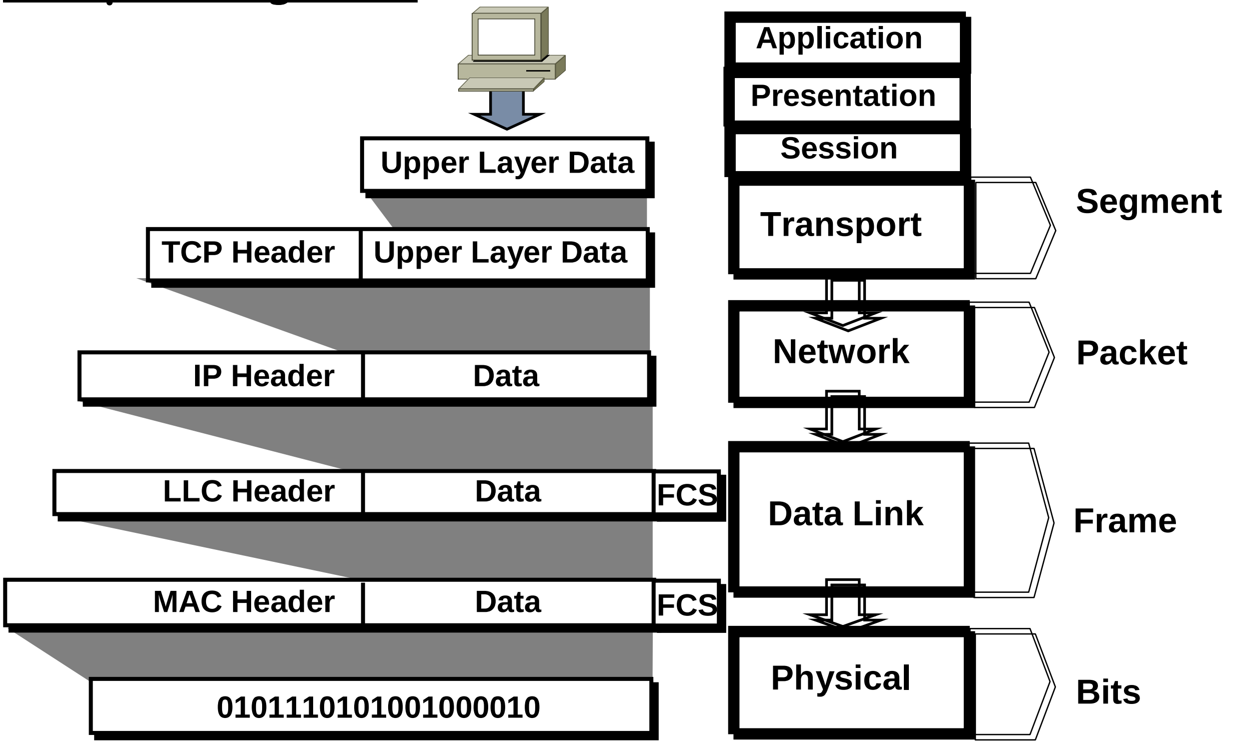
Physical

- Move bits between devices
- Specifies voltage, wire speed and pin-out cables

EIA/TIA-232
V.35

This figure reviews the entire OSI model stack.

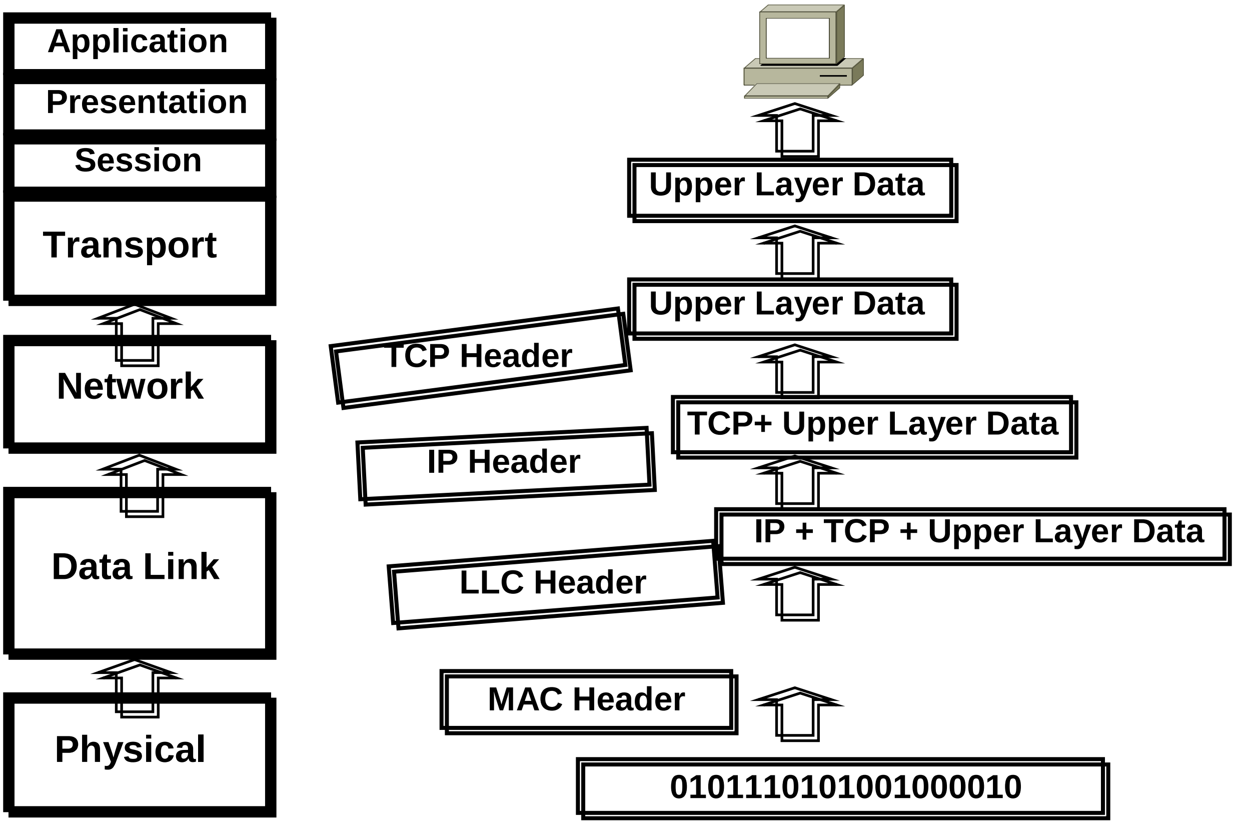
Encapsulating Data



The protocol data units (PDUs) are the terms used in the industry and in this bookto describe data at the different layers .

Encapuslation is a key concept that illustrates how data is formatted prior to being sent across a link. This example is an illustration is Ethernet (or token ring) at the data link and physical layer and TCP/IP at the network and transport layers

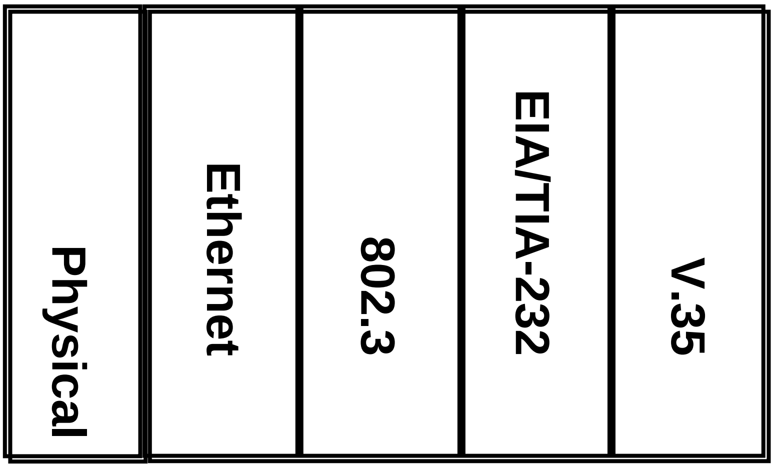
De-encapsulating Data



At the destination, the headers at each layer are stripped off as the data moves back up the stack .

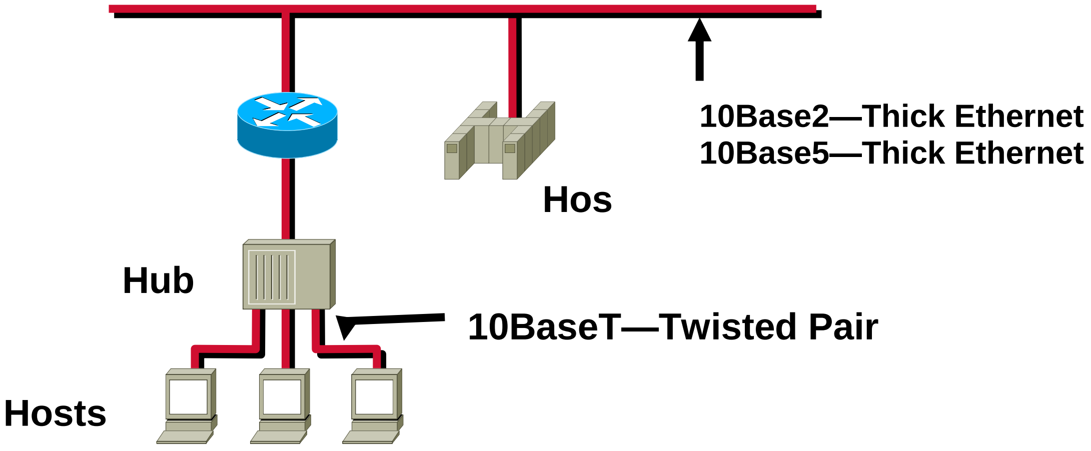
Physical Layer Functions

Defines
*Media type
*Connector type
*Signaling type



Note: 802.3 is responsible for LANs based on the carrier sense multiple access collision detect (CSMA/CD) access methodology. Ethernet is an example of a CSMA/CD network.
EIA/TIA-232 and V ٣٥.are physical standards that support synchronous serial.

Physical Layer: Ethernet/802.3

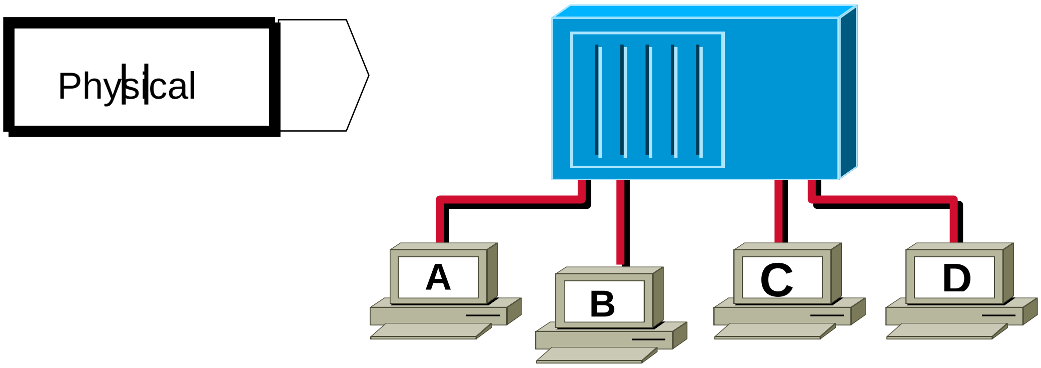


Network topology is not necessarily connected to network technology. For example, many Ethernet networks have a backbone bus topology. However, adding a switch or a hub to an Ethernet network changes it to a star topology.

IEEE 802.3u defines the standard for a CSMA/CD LAN operating at 100Mbps, Fast Ethernet.

In the case of Ethernet, such as 10BaseT, the first part describes the speed of the cable, the second part describes whether it is baseband or broadband cable, the final part describes the media. So, 10BaseT is 10 Mbps baseband twisted-pair cable.

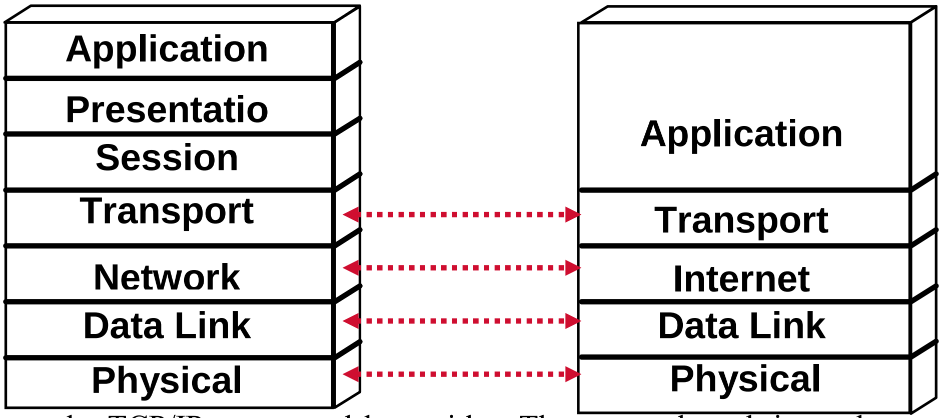
Hubs Operate at Physical layer



- All devices in the same collision domain
- All devices in the same broadcast domain
- Devices share the same bandwidth

All devices attached to a hub are on the same collision and broadcast domain. A hub is a layer one device.

TCP/IP Protocol Stack

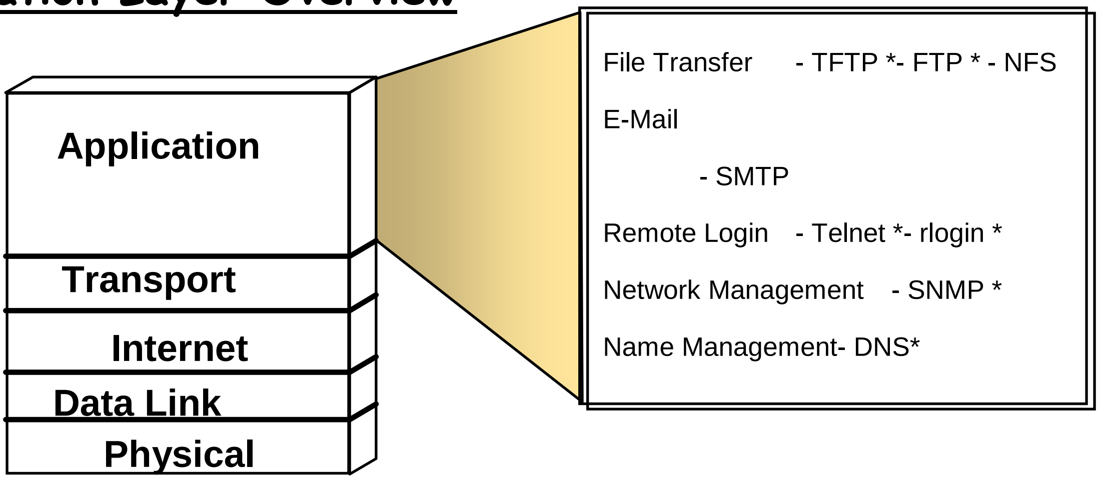


This figure shows the TCP/IP conceptual layer titles. The protocol stack is used several times in this chapter, and the lower two layers may be sometimes called the network interface layer.

The terms "packet" and "datagram" are nearly interchangeable. However, a datagram is a unit of data, while a packet is a physical entity that appears on a network. In most cases, a packet contains a datagram. In some protocols, though, a datagram is divided into a number of packets to accommodate a requirement for smaller transmittable pieces.

Note: Creation and documentation of the Internet protocols closely resembles an academic research project .The protocols are specified in documents called RFCs. RFCs are published, reviewed, and analyzed by the Internet community

Application Layer Overview


Application
Transport
Internet
Data Link
Physical
File Transfer - TFTP *- FTP * - NFS
E-Mail
- SMTP
Remote Login - Telnet *- rlogin *
Network Management - SNMP *
Name Management- DNS*

The common network applications today include file transfer, remote login, network management, and e-mail.

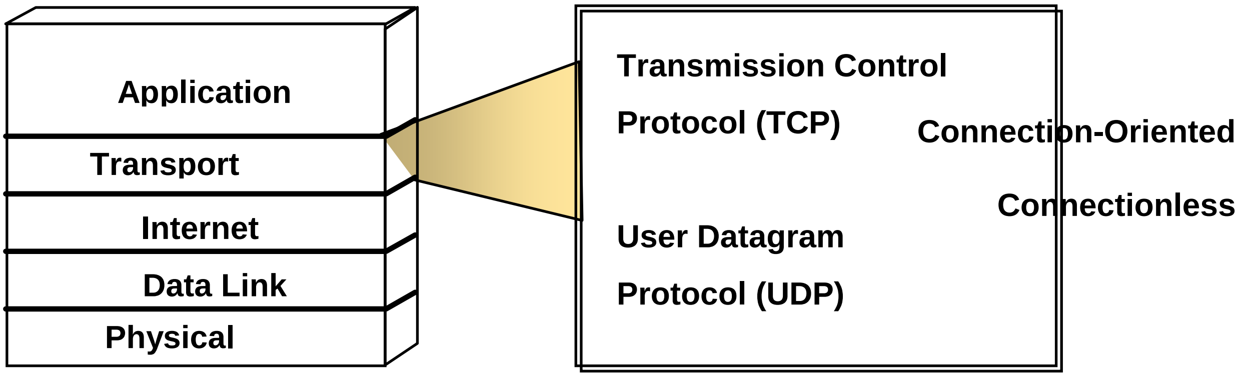
We focus on TCP/IP in this course for several reasons :

TCP/IP is a universally available protocol and you will use it at work .

TCP/IP is a useful reference for understanding other protocols, because it includes elements that are representative of other protocols .

TCP/IP is important because the router uses it as a configuration tool. The router uses Telnet for remote configuration, TFTP to transfer configuration files and operating system images, and SNMP for network management

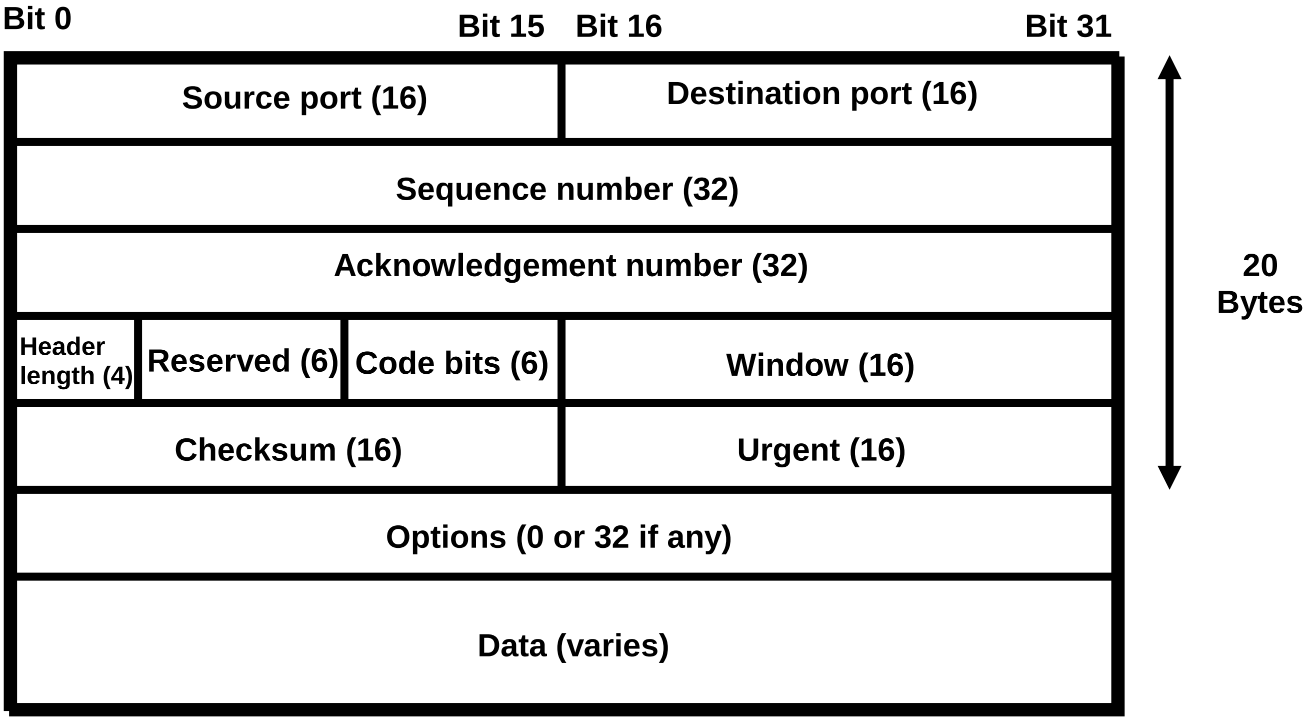
Transport Layer Overview



TCP is one protocol within the protocol suite of TCP/IP. TCP is an acknowledged transport-layer protocol. However, TCP has a large header so there is much overhead.

UDP is unacknowledged. By eliminating all of the acknowledgement mechanisms, UDP is fast and efficient. UDP does not divide application data into pieces. Reliability is assumed to be handled by the upper-layer protocols, by a reliable lower-layer protocol, or by an error-tolerant application. UDP does have a smaller header and less overhead.

TCP Segment Format



Source Port and Destination Port are the connections to the upper-layer protocol.

Sequence and Acknowledgment numbers are the position in the user's byte stream of this segment . Sequence numbers are used for establishing reliability.

HLEN is the header length. It tells us where the data begins.

Six bits are reserved for future use.

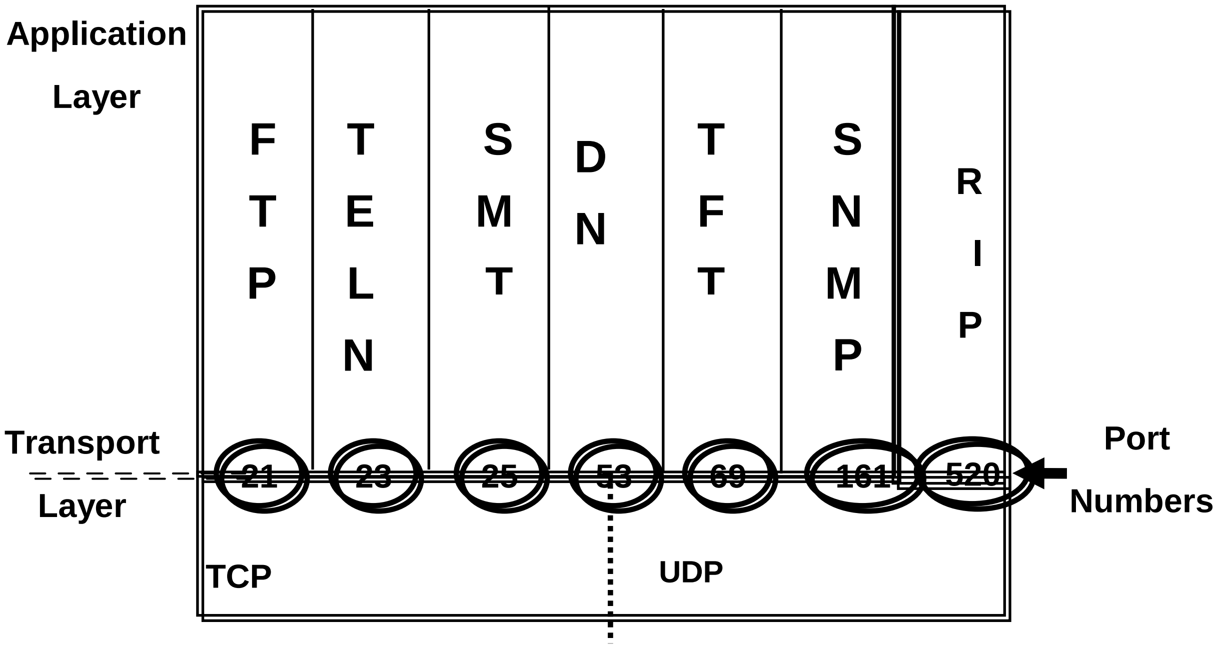
Code Bits distinguish session management messages from data.

Window is a term we will come back to in a few slides. For now, consider it the size of the receivers buffers.

Checksum is a cyclic redundancy check (CRC). It verifies that the datagram arrived intact.

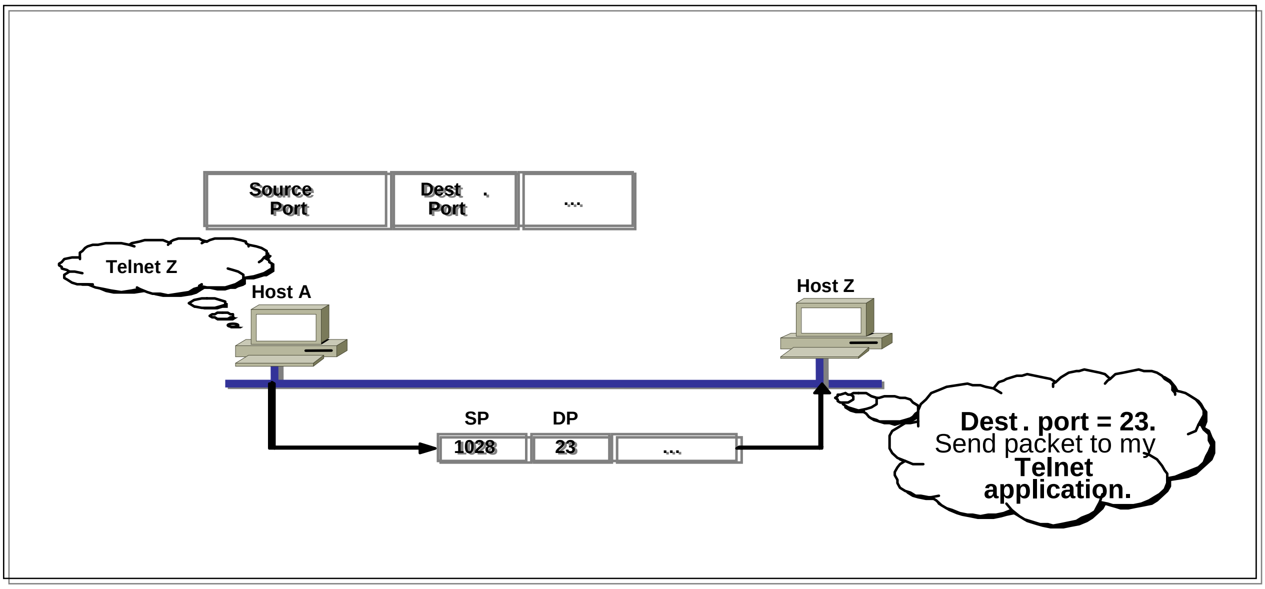
Urgent Pointer is used to signify out-of-band data.
Options are used by vendors to enhance their protocol offering.
The data portion of the frame contains the upper-layer protocol data.

Port Numbers



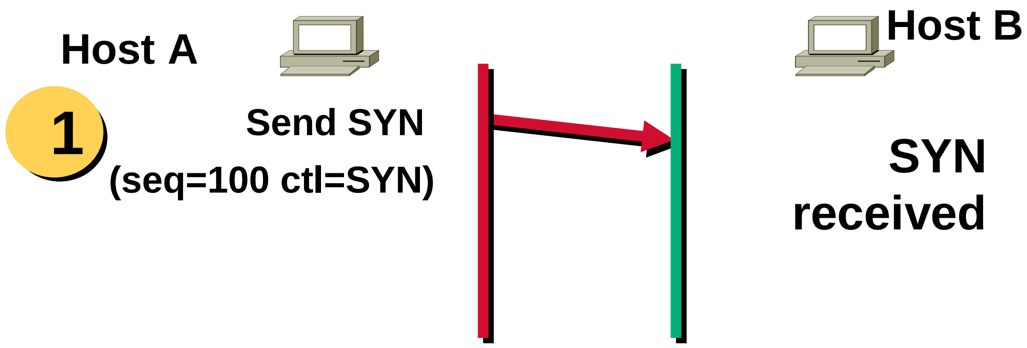
These port numbers were standardized in RFC 1340. This RFC has been obsoleted by RFC 1700. However, many of the port numbers outlined in RFC 1340 are still being used as standards .
It is possible to filter on TCP port numbers.
The TCP port number, combined with other information, is what UNIX C language developers call a socket. However, work sockets have different meanings in XNS and Novell, where they are service access point abstractions or programming interfaces rather than service access point identifiers

TCP Port Numbers



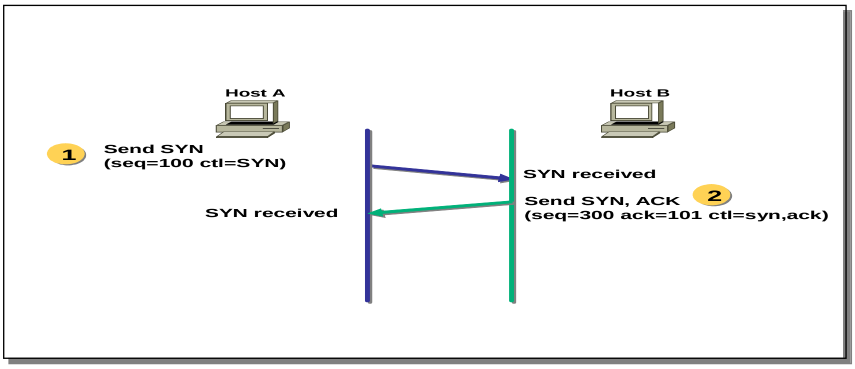
In most cases the TCP port number on one side of a conversation is the same on the other side. For example, when a file transfer takes place, the software on one host is communicating with a peer application on another host.
In this example we see a Telnet (TCP port 23) session. It is possible to have multiple Telnet sessions running simultaneously on a host or router. Telnet selects an unused port number above 1023 to represent the source port for each independent session. Notice that the destination port is still 23 .
Port numbering is important to understand in order to configure IP extended access lists. The lack of symmetry in port number use is a critical factor in establishing effective security

TCP Three Way Handshake/Open Connection



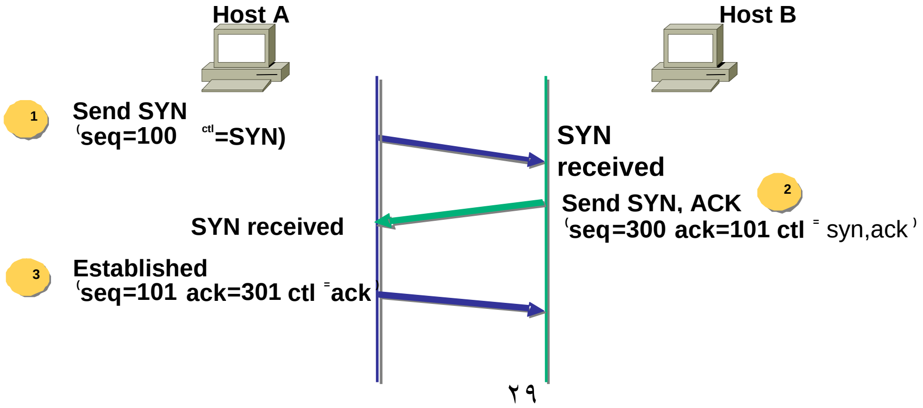
TCP is a simple protocol in terms of connection establishment. Some protocols have dozens of negotiation messages that are transmitted prior to session initialization.
TCP implements a strategy that is both necessary and sufficient..

TCP Three Way Handshake/Open Connection



Host B sends an ACK and acknowledges the SYN it received from host A. Host B also sends a SYN. Note that the acknowledgment field indicates host B is now expecting to hear sequence 101, acknowledging the SYN that occupied sequence 100.

TCP Three Way Handshake/Open Connection

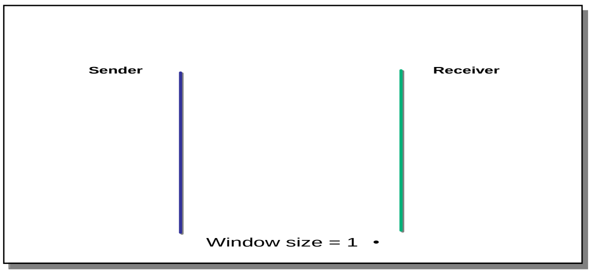


This sequence is like two people talking. The first person wants to talk to the second, so she says, “I would like to talk with you.” (SYN.) The second person responds, “Good. I want to talk with you.” (SYN, ACK.) The first person then says, “Fine—let us talk. Here is what I have to say.” (SYN, ACK, DATA(.

At this point either side can begin communicating and either side can break the connection. TCP is a peer-to-peer (balanced) communication method (no primary/secondary .(

Note: This figure explains TCP connection establishment. For more information regarding the three-way handshake in establishing a TCP connection, refer to RFC 793.

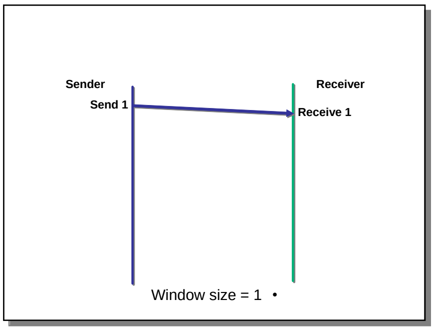
TCP Simple Acknowledgment

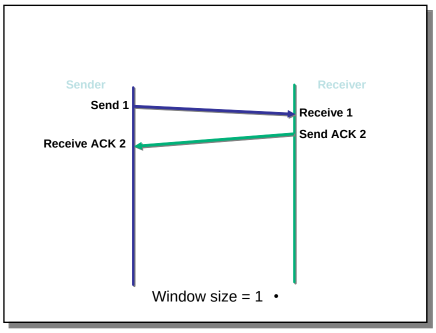


The window size is the number of messages transmitted before the sender must wait for an acknowledgment. Window size was presented earlier in the course, so this slide is a review.

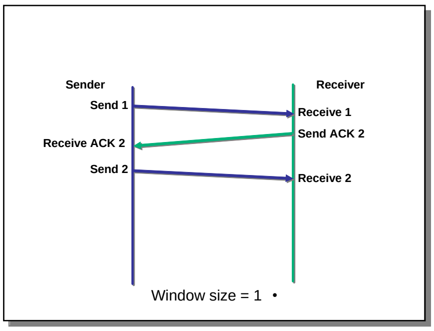
The initial state, no messages being sent.

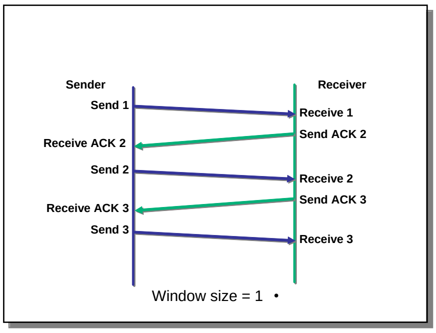
TCP Simple Acknowledgment





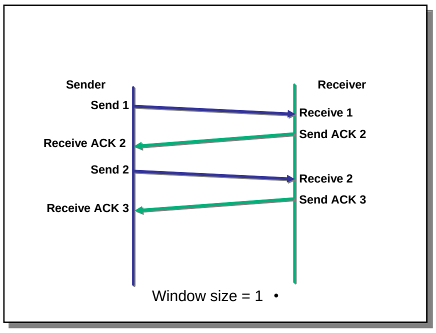
Data message 1 sent. (Send 1, Receive 1) (Acknowledgment message 2 sent. (Send ACK 2, Receive ACK 2)



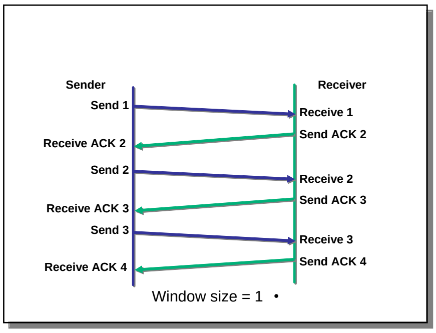


Data message 2 sent. (Send 2, Receive 2(

Send 3, Receive 3.



ACK for message 2. (Send ACK 3, Receive ACK 3(



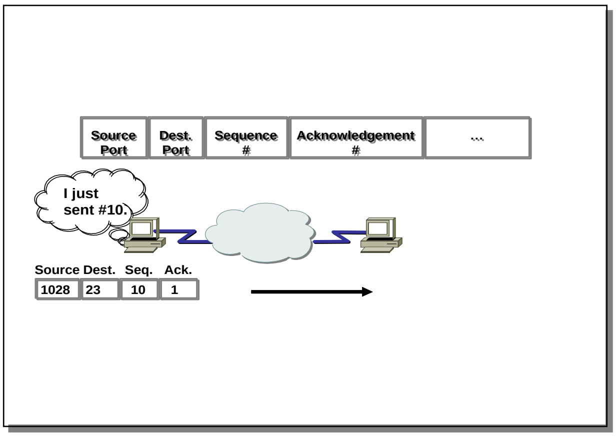
ACK for message 3. (Send ACK 4, Receive ACK 4(

This sequence helps to convey the delay associated with a window size of one.

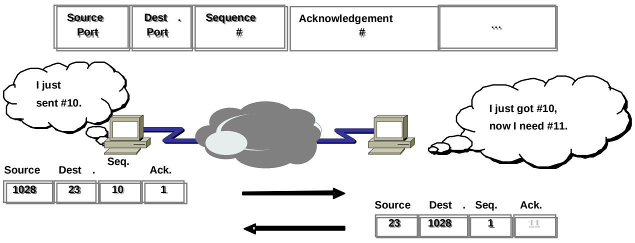
Note: TCP acknowledgments are expectational and are sometimes called forward referenced, which means that they refer to the segment they are expecting to receive, not the one just sent.

Acknowledgment field sizes can become an issue when transmitting data at FDDI and ATM speeds.

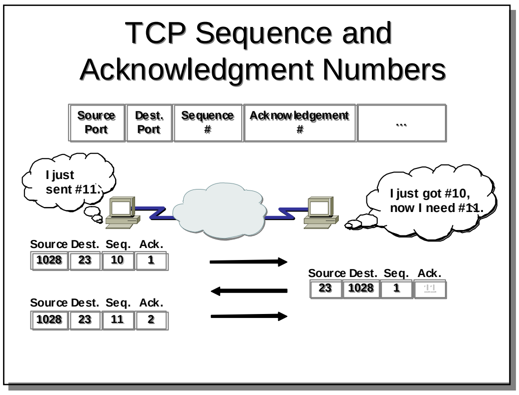
TCP Sequence and Acknowledgment Numbers



Layer 1 shows the Sequence number is 1.

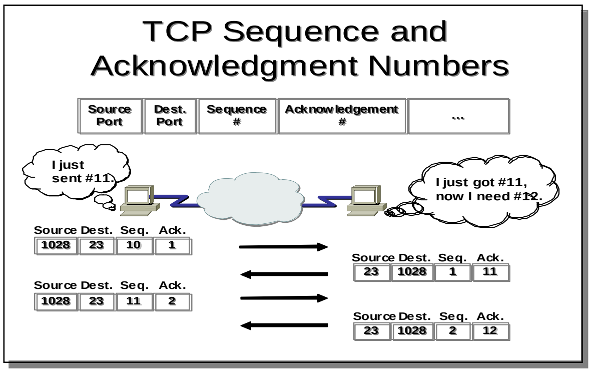


Layer 2 shows the acknowledgment number is 11.



TCP Sequence and Acknowledgment Numbers

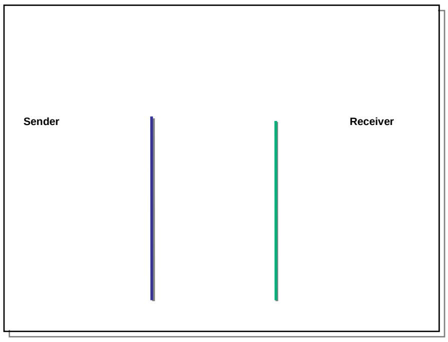
Layer 3 shows the next sequence .number is 11



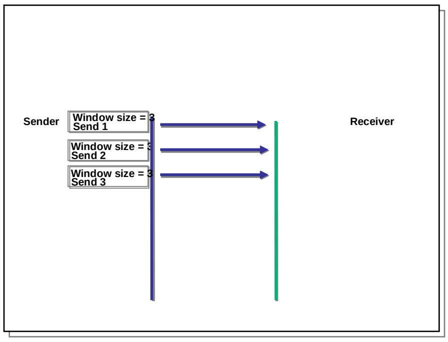
TCP Sequence and Acknowledgment Numbers

The Sequence and Acknowledgment numbers are directional. The slide highlights the communication going in one direction. The sequence and acknowledgments take place with the sender on the right. TCP provides full-duplex communication.

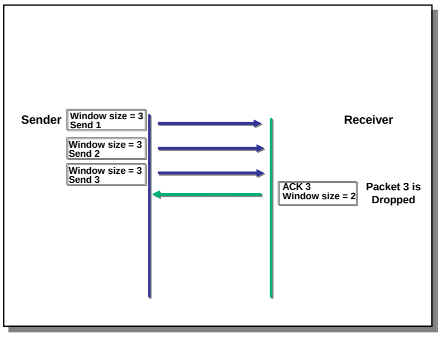
TCP Windowing



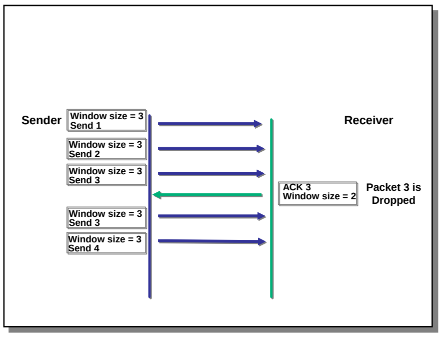
This figure points out the benefit of a larger window size. Layer 1 is in the initial state, no messages being sent.



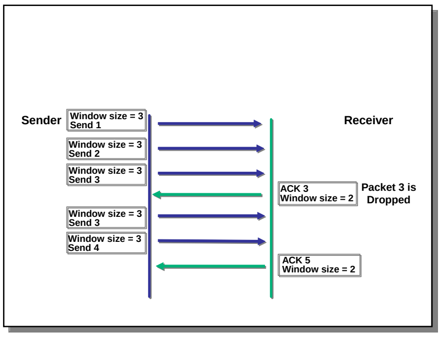
Layer 2 illustrates how the sending device defines its window buffer as 3 and sends three bytes



In layer 3, the receiving device acknowledges the two first bytes, drops 3, and advertises its window size as 2.

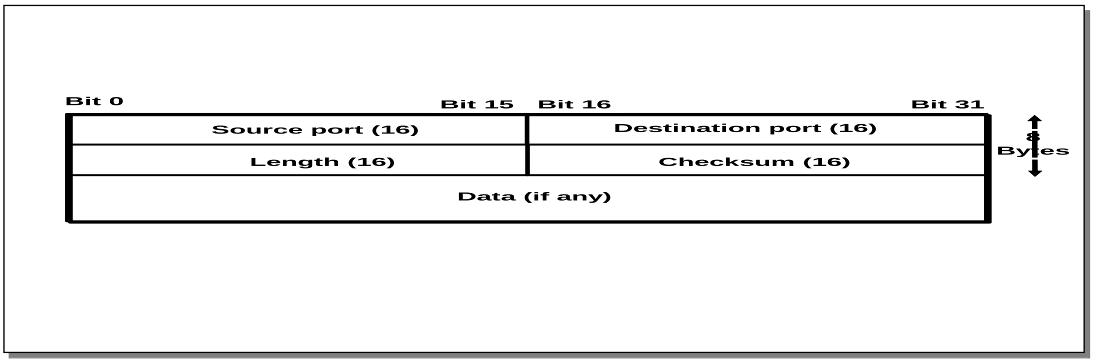


In layer 3 the sending device transmits 2 bytes but maintains a window size of 2.



In layer 5, the receiving device acknowledges the 2 bytes and still advertises its window size as 2.

UDP Segment Format


Bit 0 | Bit 15 | Bit 16 | Bit 31

Bit 0 … Bit 15	Bit 16 … Bit 31
Source port (16)	Destination port (16)
Length (16)	Checksum (16)
Data (if any)	

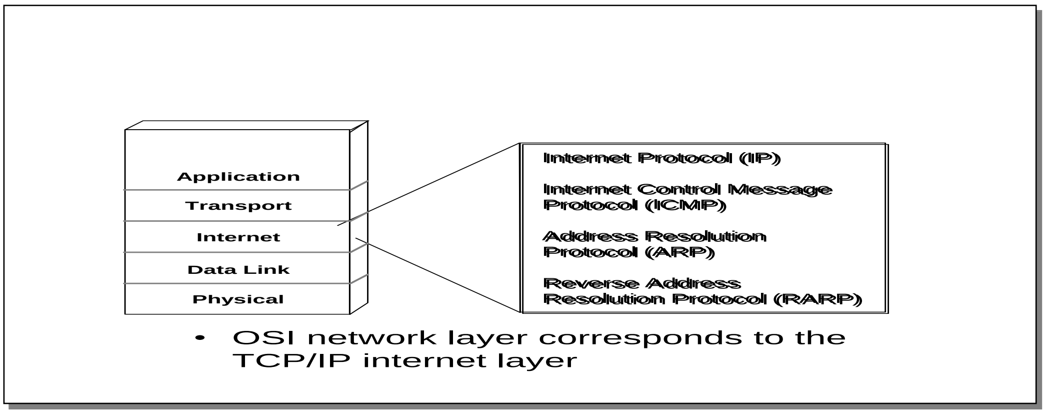
8 Bytes

UDP is simple and efficient but not reliable. The UDP segment format includes a source port, a destination port, a length field, and an optional checksum field. It has no sequencing, acknowledgments, or windowing.

Example: TFTP uses a checksum. At the end of the transfer if the checksum does not match then the file did not make it. The user is notified and must type in the command again. As a result, the user has become the reliability mechanism.

Transition: The next section discusses the network layer of the OSI model and how it corresponds to the TCP/IP internet layer.

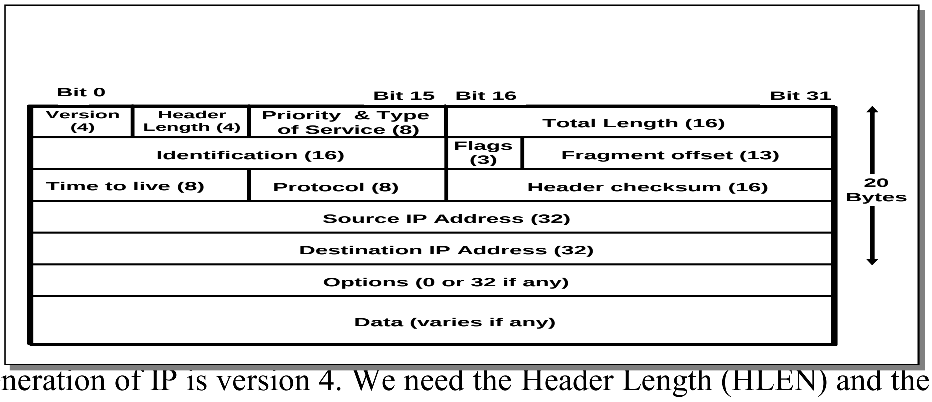
Internet Layer Overview


Application
Transport
Internet
Data Link
Physical
Internet Protocol (IP)
Internet Control Message Protocol (ICMP)
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)

- OSI network layer corresponds to the TCP/IP internet layer

Routing protocols are usually considered layer-management protocols that support the network layer .

IP Datagram


Bit 0 | Bit 15 | Bit 16 | Bit 31

Version (4)	Header Length (4)	Priority & Type of Service (8)	Total Length (16)	
Identification (16)			Flags (3)	Fragment offset (13)
Time to live (8)		Protocol (8)	Header checksum (16)	
Source IP Address (32)				
Destination IP Address (32)				
Options (0 or 32 if any)				
Data (varies if any)				

20 Bytes

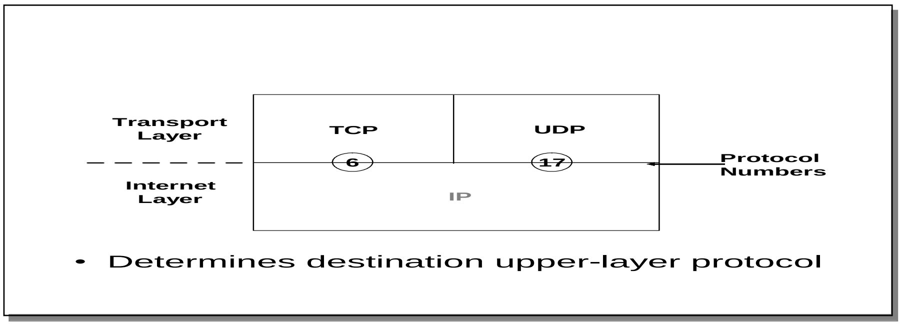
The current generation of IP is version 4. We need the Header Length (HLEN) and the Total Length in this example because the IP Options field allows a variable length .

Time-To-Live (TTL) is a countdown field. Every station must decrement this number by one or by the number of seconds it holds onto the packet. When the counter reaches zero, the time to live expires and the packet is dropped. TTL keeps packets from endlessly wandering the internet in search of nonexistent destinations.

The next generation of IP (called IPng) is IP version 6. It is covered in RFC 1752.

Good references for this topic are Douglas Comer's books on TCP/IP.

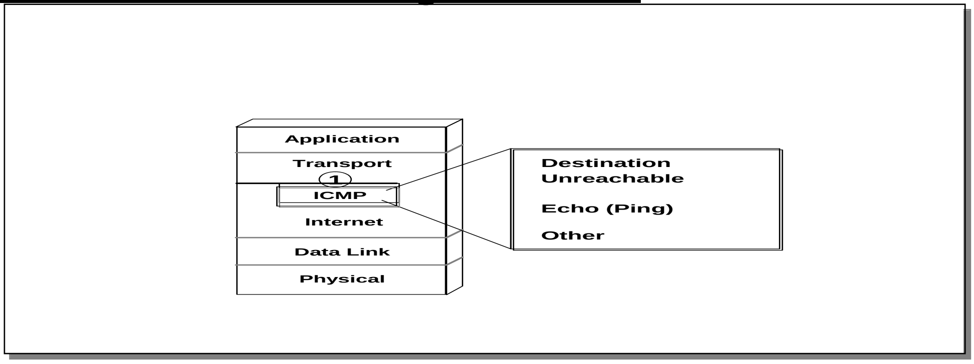
Protocol Field



- Determines destination upper-layer protocol

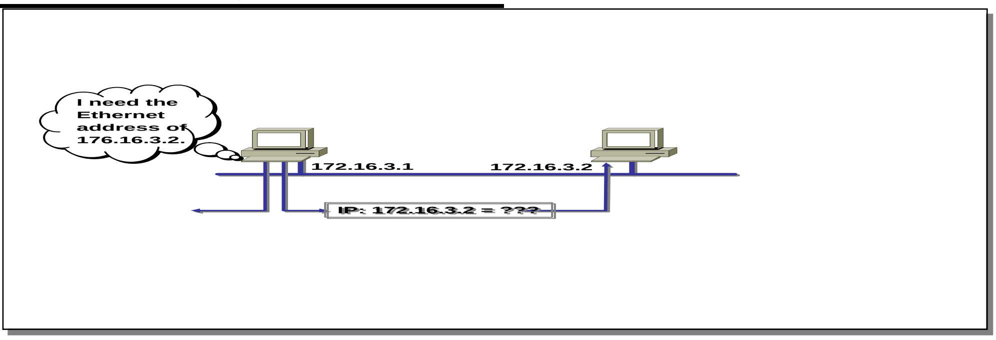
Protocol numbers connect, or multiplex, IP to the transport layer. These numbers are standardized in RFC 1700. Cisco uses these numbers in filtering with extended access lists.

Internet Control Message Protocol



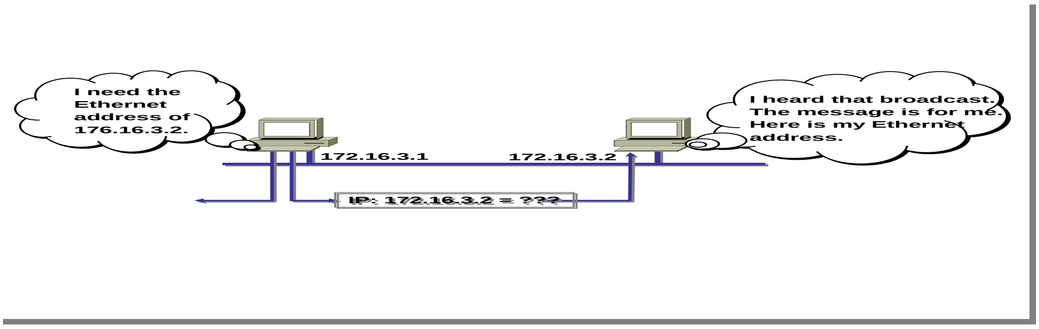
Describe ICMP messages and ping

Address Resolution Protocol

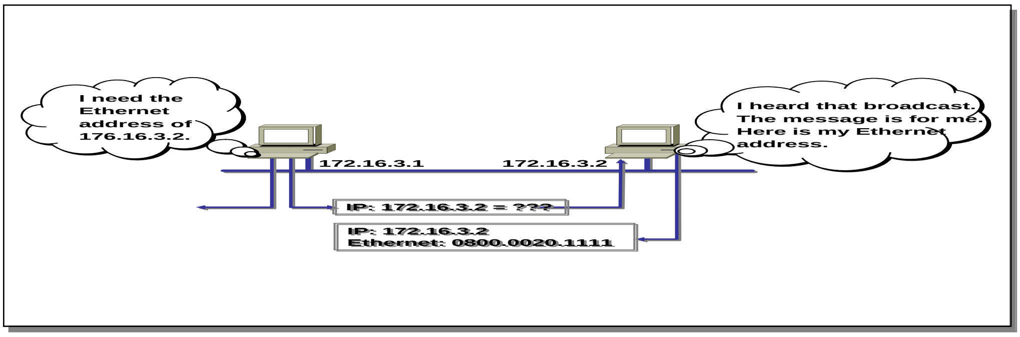


This figure shows how ARP is used to determine an IP address.

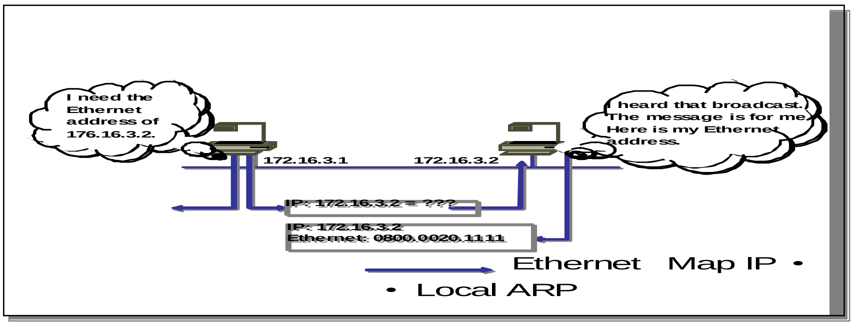
In layer 1, host 172.16.3.1 needs the MAC address of host 172.16.3.2. It sends an ARP request message


I need the Ethernet address of 176.16.3.2.
I heard that broadcast. The message is for me. Here is my Ethernet address.
172.16.3.1
172.16.3.2
IP: 172.16.3.2 = ???

host 172.16.3.2 is on the same wire and receives the ARP request message

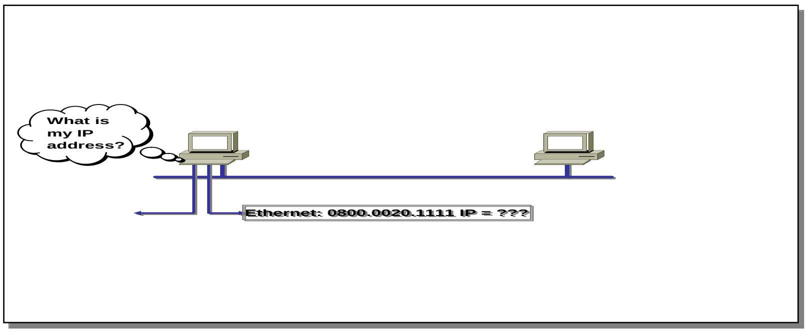

I need the Ethernet address of 176.16.3.2.
I heard that broadcast. The message is for me. Here is my Ethernet address.
172.16.3.1
172.16.3.2
IP: 172.16.3.2 = ???
IP: 172.16.3.2
Ethernet: 0800.0020.1111

host 172.16.3.2 sends an ARP reply with its MAC address to host 172.16.3.1.


I need the Ethernet address of 176.16.3.2.
I heard that broadcast. The message is for me. Here is my Ethernet address.
172.16.3.1
172.16.3.2
IP: 172.16.3.2 = ???
IP: 172.16.3.2
Ethernet: 0800.0020.1111
Ethernet Map IP •
• Local ARP

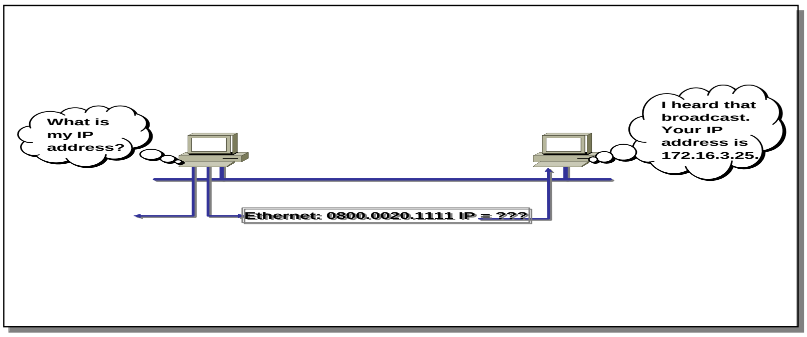
ARP provides translation between network and data link layers.
Discuss why it is necessary to have a mechanism like ARP.
Describe ARP operation.
Not all protocols use ARP. Some use other methods for address translation.
Note: For the message to be transmitted uniquely to a single interface on the multiaccess link, it is necessary to build a frame with the unique MAC address of the interface

Reverse ARP

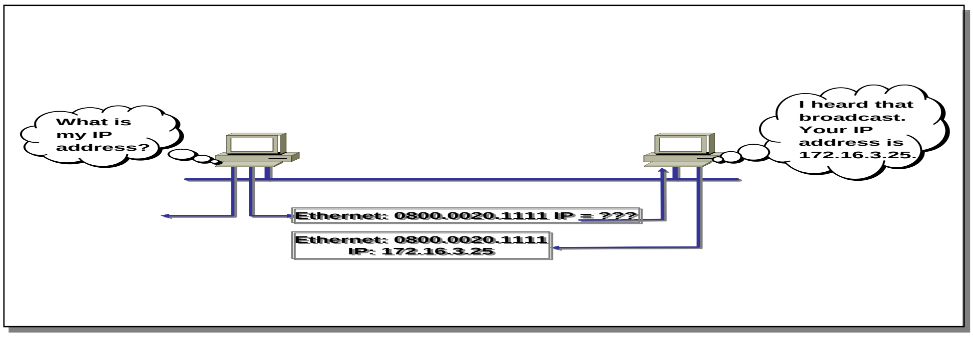


This figure explains how RARP works .

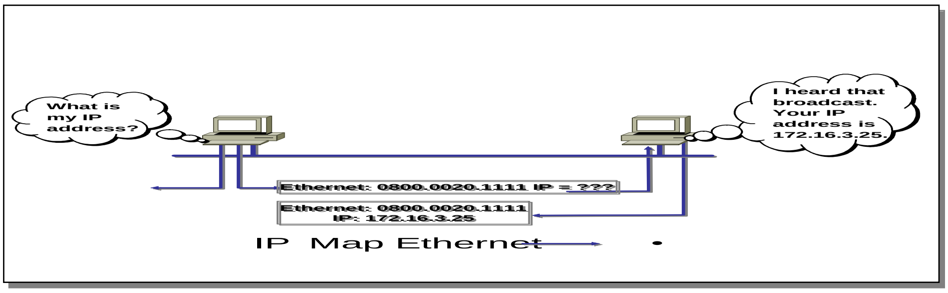
In layer 1, the host on the left needs its IP address. It sends a RARP request with its MAC address


What is my IP address?
I heard that broadcast. Your IP address is 172.16.3.25.
Ethernet: 0800.0020.1111 IP = ???

the host on the right, functioning as a RARP server, maps the MAC address to an IP address.

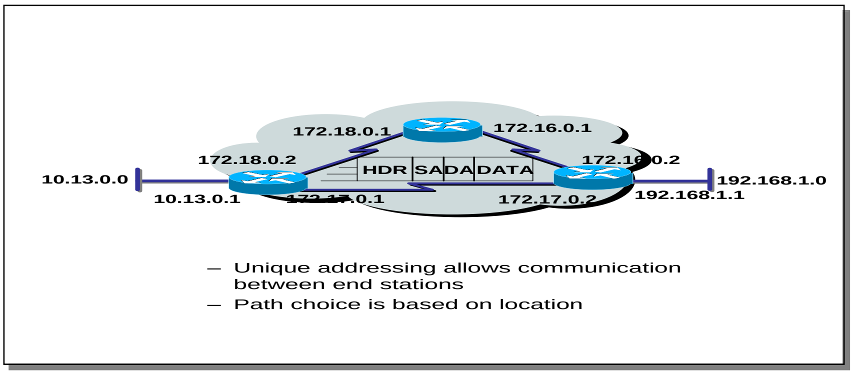

What is my IP address?
I heard that broadcast. Your IP address is 172.16.3.25.
Ethernet: 0800.0020.1111 IP = ???
Ethernet: 0800.0020.1111 IP: 172.16.3.25

the host on the right sends the IP address to the requester in a RARP reply message.


What is my IP address?
I heard that broadcast. Your IP address is 172.16.3.25.
Ethernet: 0800.0020.1111 IP = ???
Ethernet: 0800.0020.1111 IP: 172.16.3.25
IP Map Ethernet

RARP is used to boot diskless workstations over a network.

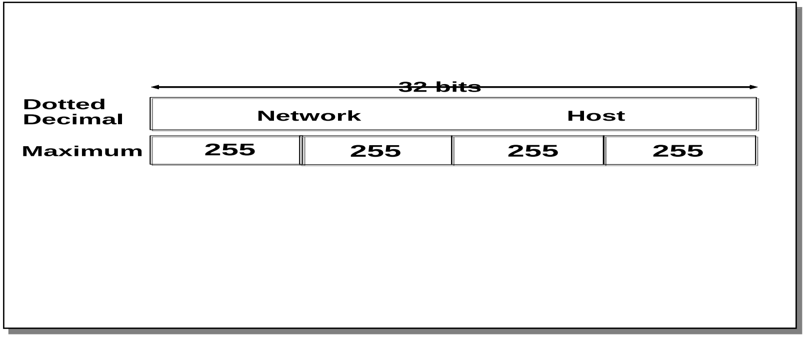
Introduction to TCP/IP Addresses



– Unique addressing allows communication between end stations
– Path choice is based on location

Stations with internetwork access must have unique addresses.

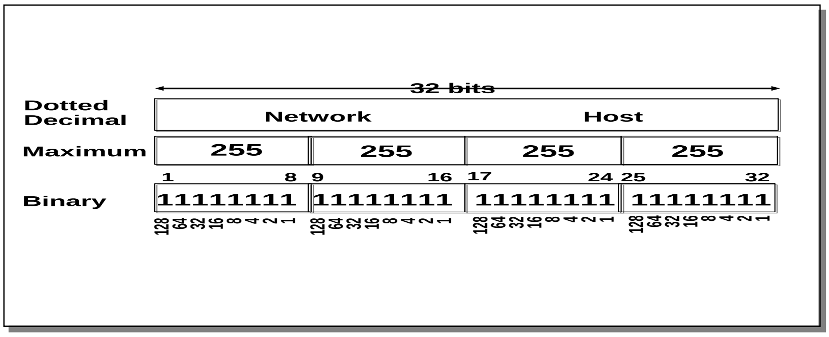
IP Addressing



	32 bits			
Dotted Decimal	Network		Host	
Maximum	255	255	255	255

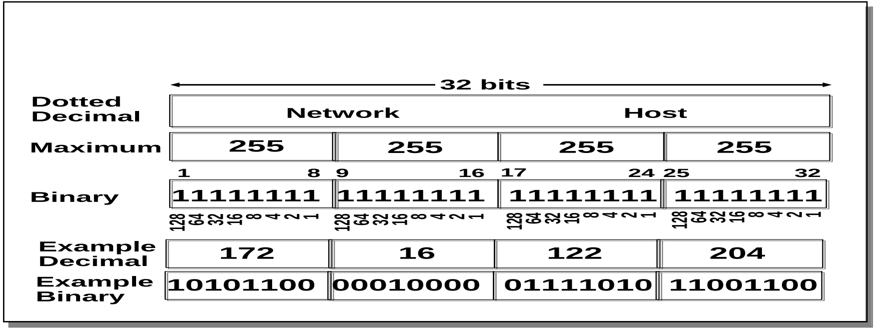
show the general format of an IP address.
the address is 32 bits with a network and host portion.

IP Addressing



	32 bits			
Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 8	9 16	17 24	25 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1

one can convert the address to binary



	32 bits			
Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 8	9 16	17 24	25 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Example Decimal	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

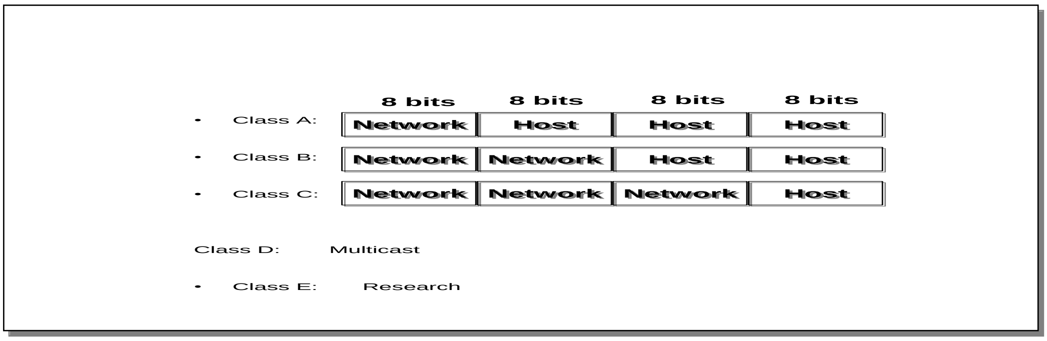
IP address format is dotted-decimal. Dotted-decimal makes it easy to work with IP addresses. However, in this course we will work with the addresses on the bit level, so we will convert these addresses into binary, make changes to them, and convert them back.

The central authority for addresses is the Internet Assigned Numbers Authority.

Note: This most common form of addressing reflects the widely used IP version 4. Faced with the problem of depleting available addresses, Internet Engineering Task Force (IETF) work is under way for a backward-compatible next generation of IP (IPng, also called IP 6 .(

IP 6 will offer expanded routing and addressing capabilities with 128-bit addresses rather than the 32-bit addressing shown on the graphic. Addresses from both IP versions will coexist. Initial occurrences will probably be at locations with address translator software and firewalls

IP Address Classes



	8 bits	8 bits	8 bits	8 bits
- Class A:	Network	Host	Host	Host
- Class B:	Network	Network	Host	Host
- Class C:	Network	Network	Network	Host

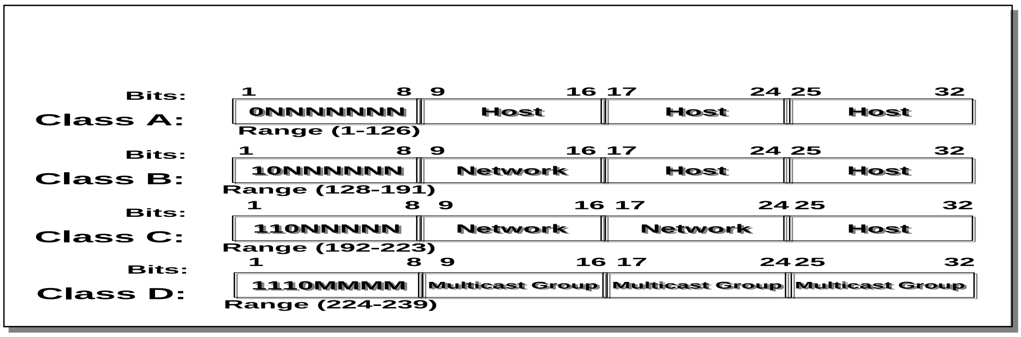
Class D: Multicast

- Class E: Research

Discuss classes of addresses. Each address contains information about the network number and the host number of the device. Class A addresses are for very large organizations. Class B addresses are for smaller organizations, and Class C addresses for even smaller ones.

As the number of networks grows, classes may eventually be replaced by another addressing mechanism, such as classless interdomain routing (CIDR). RFC ١٤٦٧، *Status of CIDR Deployment in the Internet*, presents information about CIDR. RFC 1817, *CIDR and Classful Routing,* also presents CIDR information.

IP Address Classes



Class A: Bits: 1 8 | 9 16 | 17 24 | 25 32
0NNNNNNNN | Host | Host | Host
Range (1-126)

Class B: Bits: 1 8 | 9 16 | 17 24 | 25 32
10NNNNNNN | Network | Host | Host
Range (128-191)

Class C: Bits: 1 8 | 9 16 | 17 24 | 25 32
110NNNNN | Network | Network | Host
Range (192-223)

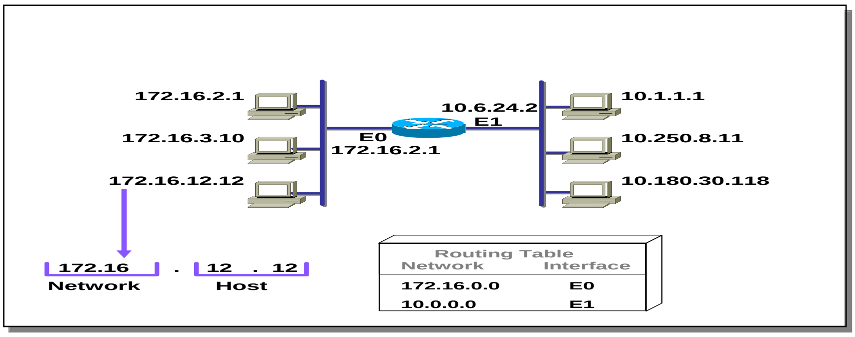
Class D: Bits: 1 8 | 9 16 | 17 24 | 25 32
1110MMMM | Multicast Group | Multicast Group | Multicast Group
Range (224-239)

Highlight the fixed values that start each class address.

The first octet rule states that when an address falls into a specified range, it belongs to a certain class. Students should soon be able to recognize the address class of any IP address on sight.

Note: If time or interest permits, you can use the initial bit patterns in the first octet and show how a class of IP network derives the range of network numbers for that IP address class.

Host Addresses

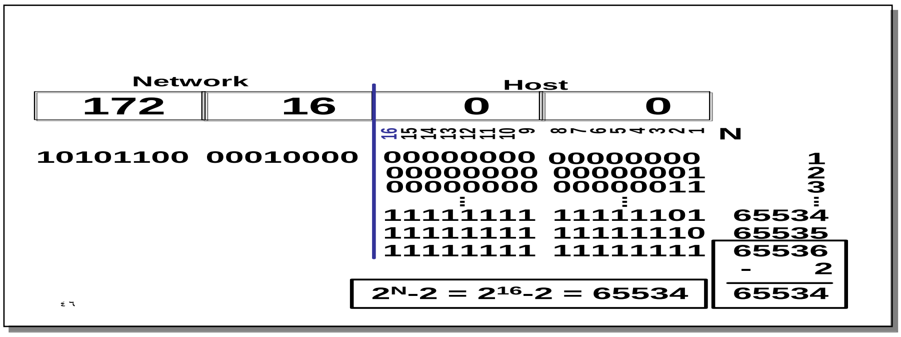


Routing Table Network	Interface
172.16.0.0	E0
10.0.0.0	E1

In the example, 172.16.0.0 and 10.0.0.0 refer to the wires at each end of the router .

Explain how the routing table is used. Entries in the routing table refer to the network only. The router does not know the location of hosts—it knows the location of networks.

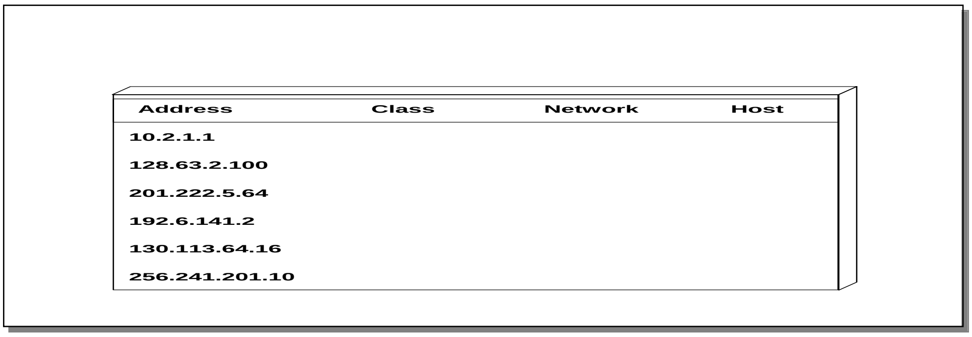
Determining Available Host Addresses



2^N-2 is the calculation to determine available hosts. N is the number of binary digits in the host field. Subtract 2 because a host cannot be all 0s or 1s.

The same principal applies when determining the number of available networks.

IP Address Classes Exercise



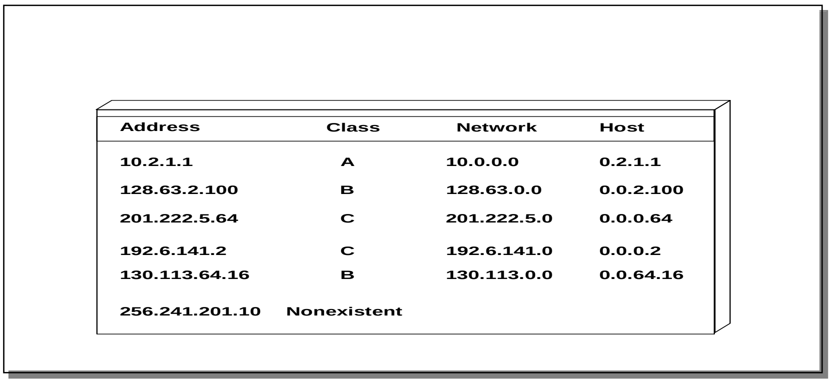
Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

This exercise verifies that the students understand IP address classes, network numbers, and host numbers.

Give the students time to list the address class, network, and host number for each IP address in the table. Review the correct answers interactively.

The answers are given in the following figure

IP Address Classes Exercise Answers

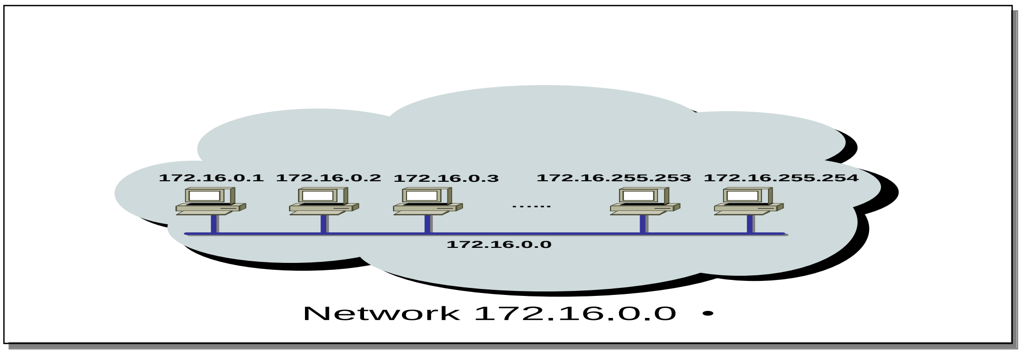


Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
256.241.201.10	Nonexistent		

This answers to the exercise are given in the figure.

Note: Students can also find the answers to this exercise in the “Answers” appendix .

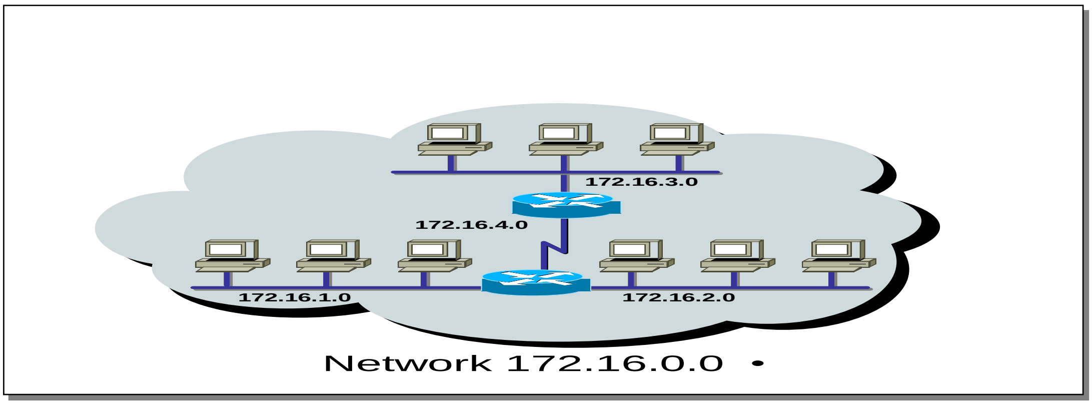
Addressing without Subnets



This figure explains what networks look like without subnets.
Without subnets, use of network addressing space is inefficient .
The Class B network is like a highway with no exits—there is no place to exit, so all of the traffic is in one line

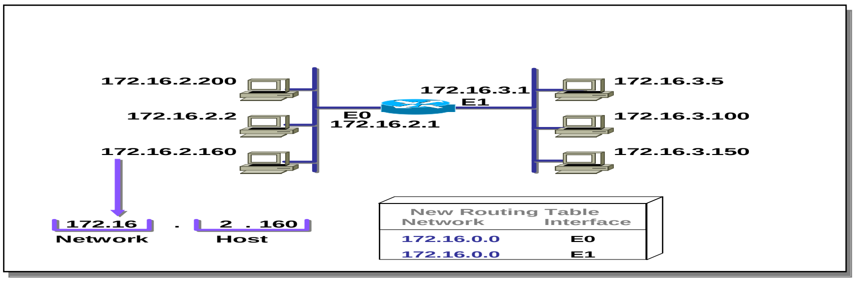
Addressing with Subnets

.



The host bits of an IP address can be subdivided into a subnetwork section and a host section. The subnetwork section in this example is the full third octet.
Point out the difference in the addressing between the previous slide and this slide.
A subnetted address space is like a highway with exits.
A network device uses a subnet mask to determine what part of the IP address is used for the network, the subnet, and the device ID .
A subnet mask is a 32-bit value containing a number of one bits for the network and subnet ID and a number of zero bits for the host ID .
Given its own IP address and subnet mask, a device can determine if an IP packet is destined for 1) a device on its own subnet, 2) a device on a different subnet on its own network, or 3) a device on a different network .
A device can determine what class of address the device has been assigned from its own IP address. The subnet mask then tells the device where the boundary is between the subnet ID and the host ID.

Subnet Addressing



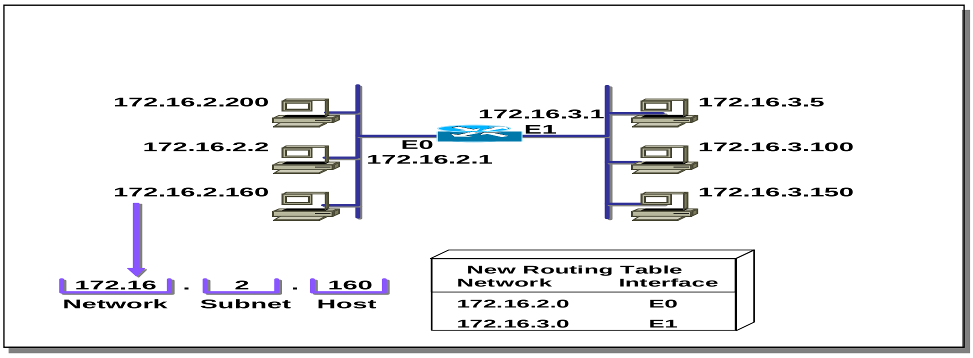
New Routing Table

Network	Interface
172.16.0.0	E0
172.16.0.0	E1

If networks could not be broken down into more granular, subnetworks few networks could exist, each with a capacity for many hosts

Subnet Addressing

.



New Routing Table

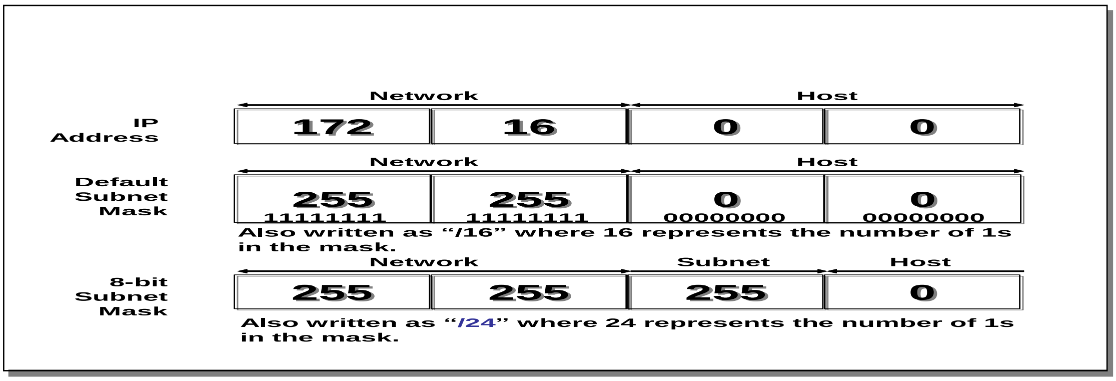
Network	Interface
172.16.2.0	E0
172.16.3.0	E1

By turning on more bits in the mask, we reserve some bits as network information and can use these bits to describe subnetworks .

Describe how the router makes use of this technique. Point out that there is more information in the routing table now.

Note: As you enter the discussion about subnet masks, a question might arise about whether it is legal to define a discontiguous subnet mask. A discontiguous subnet mask consists of intervening zeros, as in 101111011000, rather than all ones followed by zeros, as in 1111111100000000. The question has two answers. According to RFC 950 that describes IP, a discontiguous subnet mask is legal. However, the hardware expense to produce an interface that supports discontiguous masking is cost-prohibitive. Thus in practice it is not supported on most vendors' equipment, including Cisco. Also, discontiguous masking has no benefit, and it is much more difficult to maintain a network based on this design. Later RFCs make noncontiguous subnet masks illegal because they are incompatible with future addressing schemes such as CIDR.

Subnet Mask



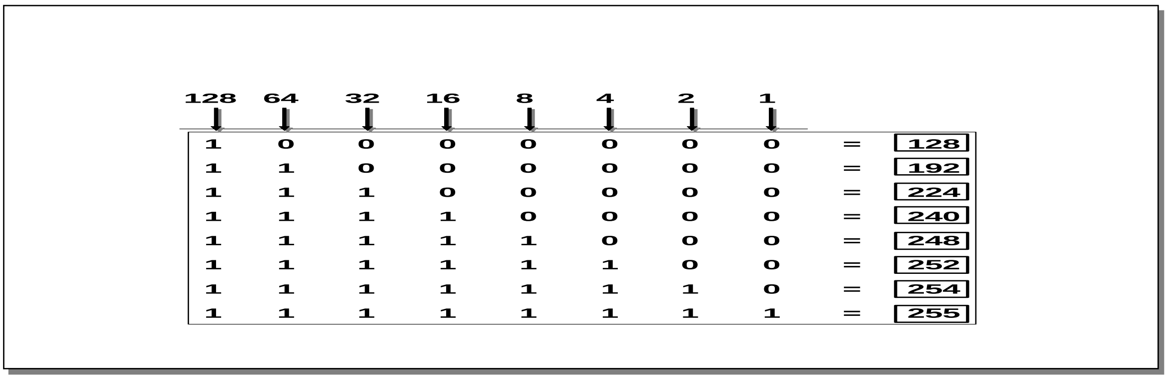
Also written as "/16" where 16 represents the number of 1s in the mask.

Also written as "/24" where 24 represents the number of 1s in the mask.

Turn on more bits to represent subnets.
Compare the default or standard subnet mask with the subnet mask in the slide.
These are the rules for IP addressing:
An address is 32 bits, divided into three components :
First octet rule bits
Network bits (path selection bits(
Node bits
The first octet rule states that the most significant bit pattern in the first octet determines the class of the address.
Path selection bits cannot be all ones or zeros.
Certain addresses are reserved. RFC 1918 defines some of those.
Prefix or mask one bits are path selection significant; zero bits are host bits and therefore not significant.
Use the logical AND to combine the address and mask bits to get the subnet address.
The maximum number of available subnets equals $2^{\text{prefix bits}}$ - 2; the maximum number of available hosts equals $2^{\text{32- prefix bits}}$

.

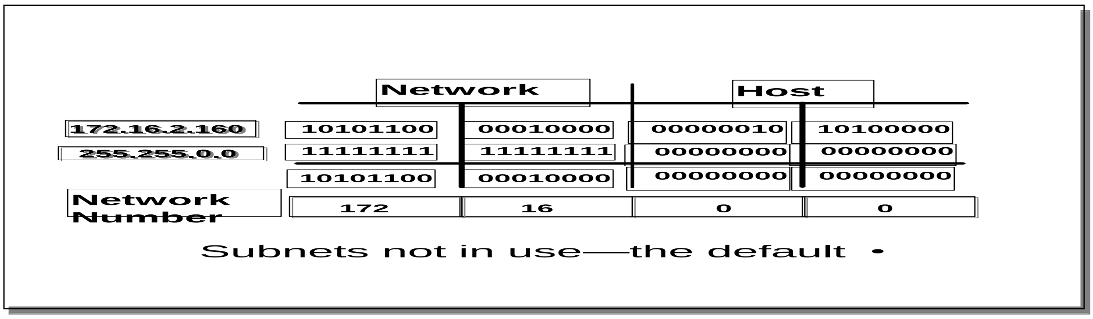
Decimal Equivalents of Bit Patterns



128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Review binary-to-decimal conversion, bit weighting, and conversion.
Explain logical AND.
One possible explanation of logical AND follows: We will need to be able to perform a logical AND on the binary numbers. Just take two binary numbers and place one above the other. The ones in the bottom are like a pipe—the number above it just drops through. The zeros are like a clogged pipe, so nothing comes out in the answer.
Presenting a truth table will help some students understand. You might need to give more than one explanation.
Note: You might want to hand out a binary-to-decimal conversion sheet if you have not already done so. We have not included one in the lab section. It is more useful to have one that is on a separate page from the labs

Subnet Mask without Subnets



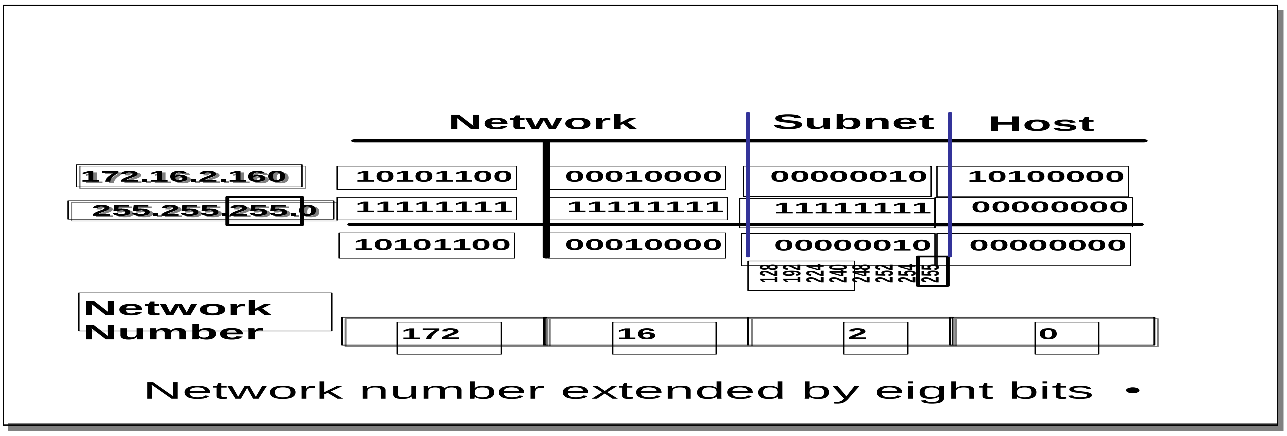
	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

Subnets not in use—the default •

Explain how masking works at the bit level. Zero bits mask host information.

Note: This is an easy place to lose students. At this point, they need to learn several abstract mathematical concepts before we can show them how to lay out an IP-addressed network. To the novice these techniques may seem unrelated, making the presentation confusing. To a more experienced audience, these techniques will be familiar.

Subnet Mask with Subnets



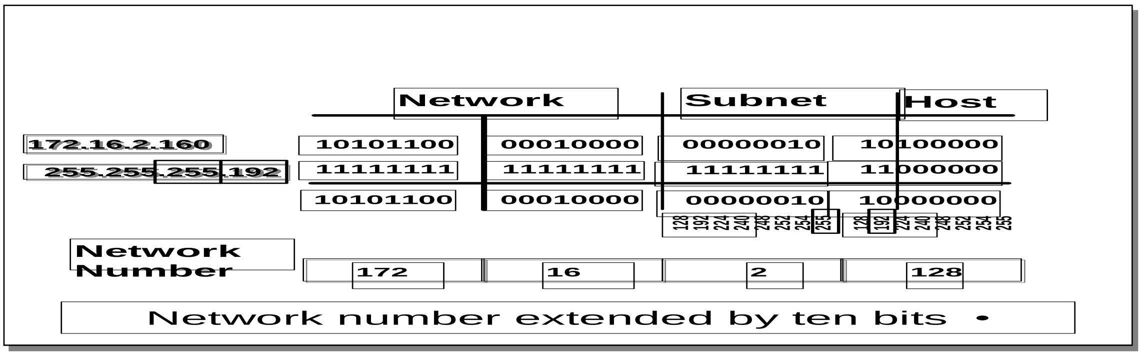
	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
			128 192 224 240 248 252 254 255	
Network Number	172	16	2	0

Network number extended by eight bits •

This example makes a Class B address space look like a collection of Class C address spaces. Now the logical AND allows us to extract the subnet number as well as the assigned network number.

An exercise follows that tests the students' understanding of subnet masks.

Subnet Mask with Subnets (cont.)

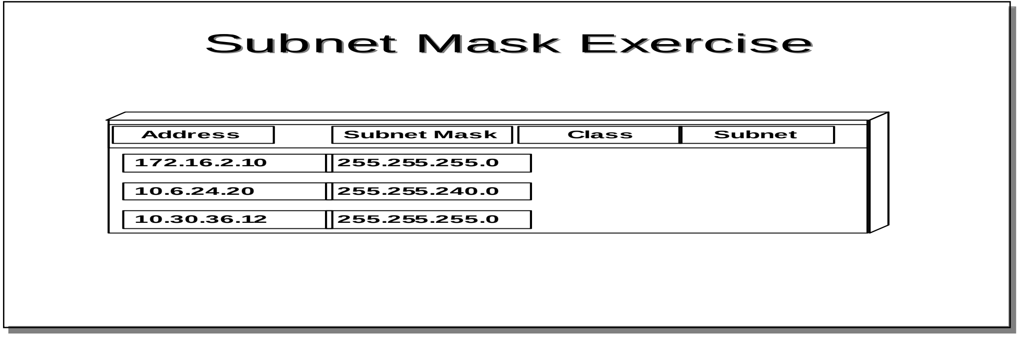


	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
			128 192 224 240 248 252 254 255	128 192 224 240 248 252 254 255
Network Number	172	16	2	128

Network number extended by ten bits •

This example is different from the previous example in that the the subnet and host are divided within an octet.

Transition: An exercise follows that tests the students' understanding of subnet masks



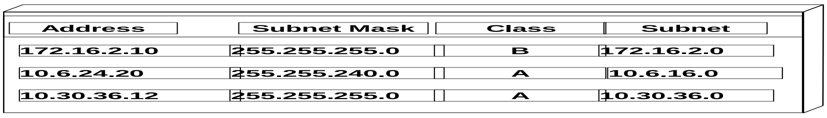
Subnet Mask Exercise

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0		
10.6.24.20	255.255.240.0		
10.30.36.12	255.255.255.0		

This exercise is for the students to take the given IP addresses and associated subnet masks and perform a logical AND to extract the subnet number. Provide time in class and review the answers after the majority of students have finished.

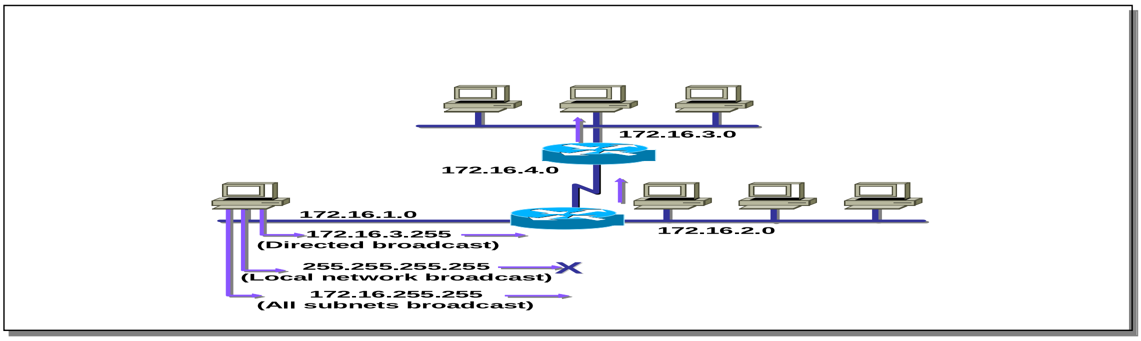
The answers are given in the following figure

Subnet Mask Exercise Answers



Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0	B	172.16.2.0
10.6.24.20	255.255.240.0	A	10.6.16.0
10.30.36.12	255.255.255.0	A	10.30.36.0

Broadcast Addresses



A range of addresses is needed to allocate address space. A valid range of addresses is between subnet zero and the directed broadcast.

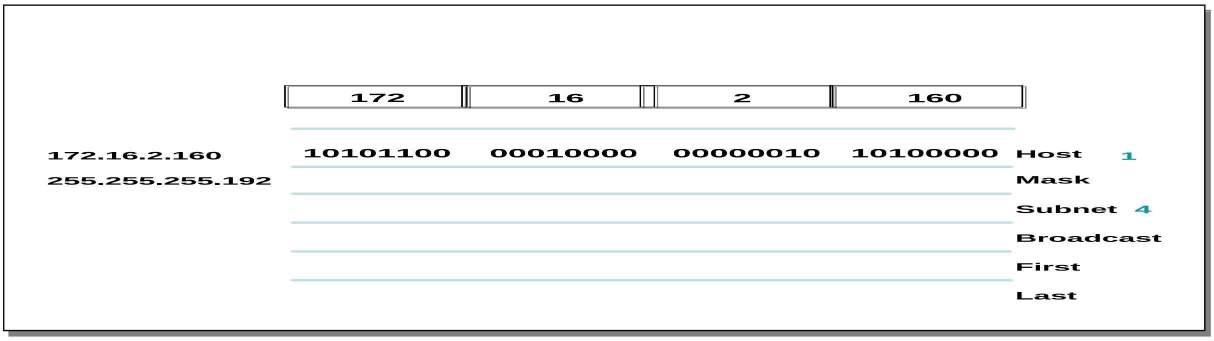
These RFCs provide more information about broadcasts:

RFC 919, *Broadcasting Internet Datagrams*

RFC 922, *Broadcasting IP Datagrams in the Presence of Subnets*

Cisco's support for broadcasts generally complies with these two RFCs. It does not support multisubnet broadcasts that are defined in RFC 922.

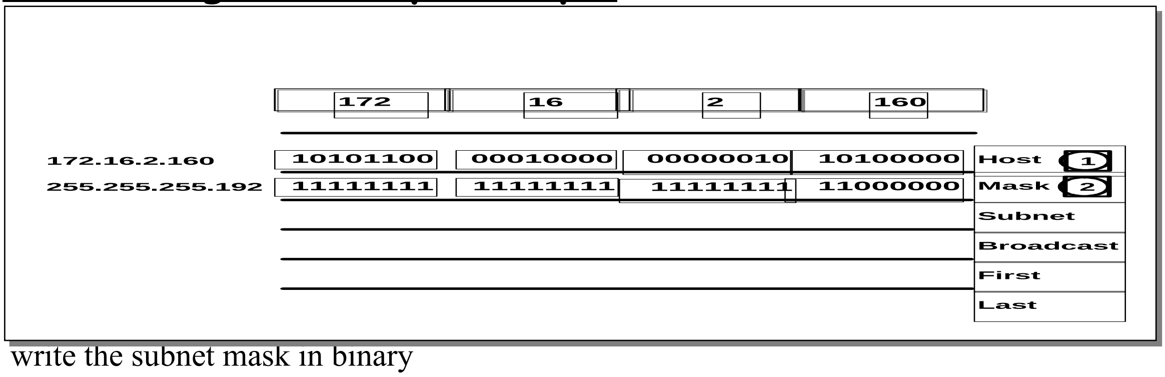
Addressing Summary Example



	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192					Mask
					Subnet 4
					Broadcast
					First
					Last

convert the address to a binary host address.

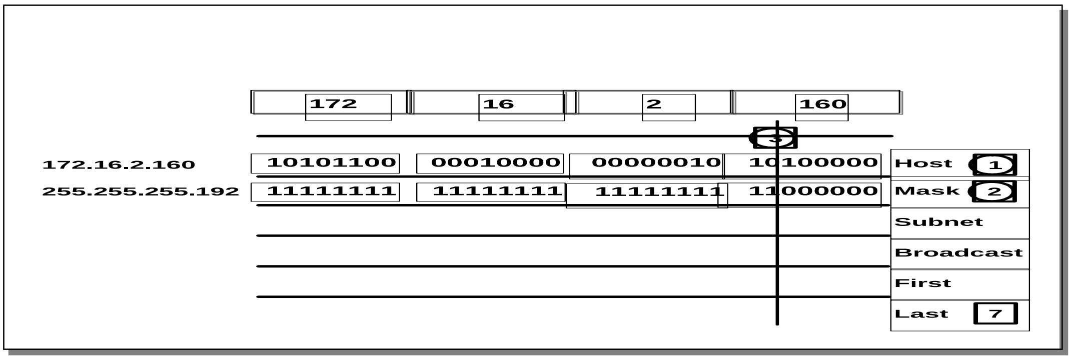
Addressing Summary Example



	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet
					Broadcast
					First
					Last

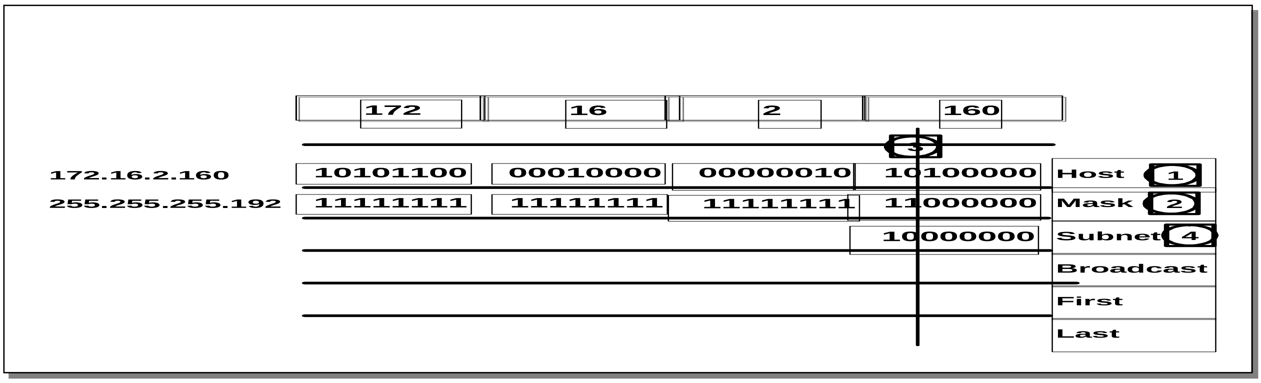
write the subnet mask in binary

Addressing Summary Example



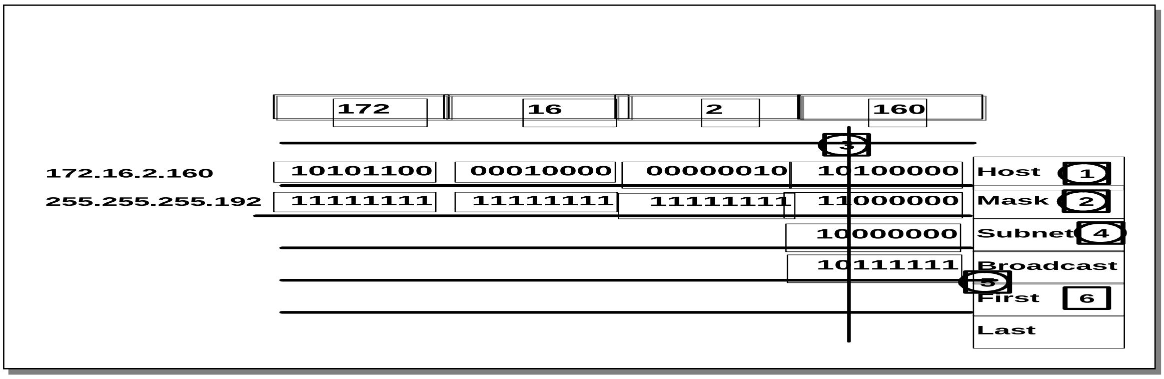
draw a line after the recursive ones in the subnet mask .

Addressing Summary



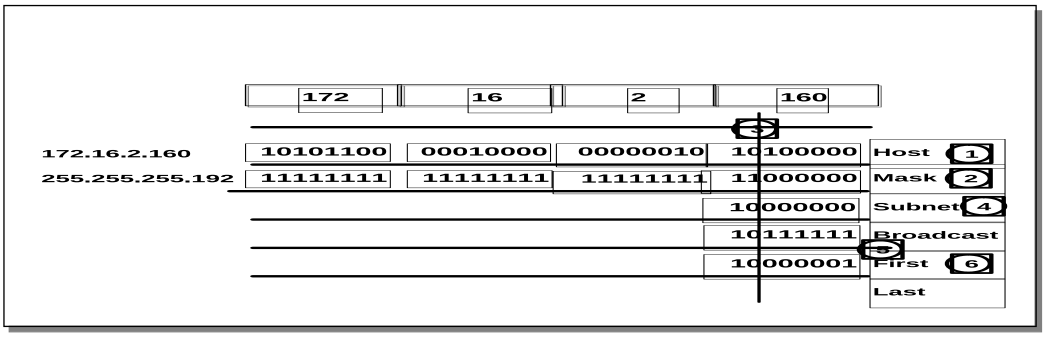
fill in zeros beyond the vertical line for the subnet.

Addressing Summary Example



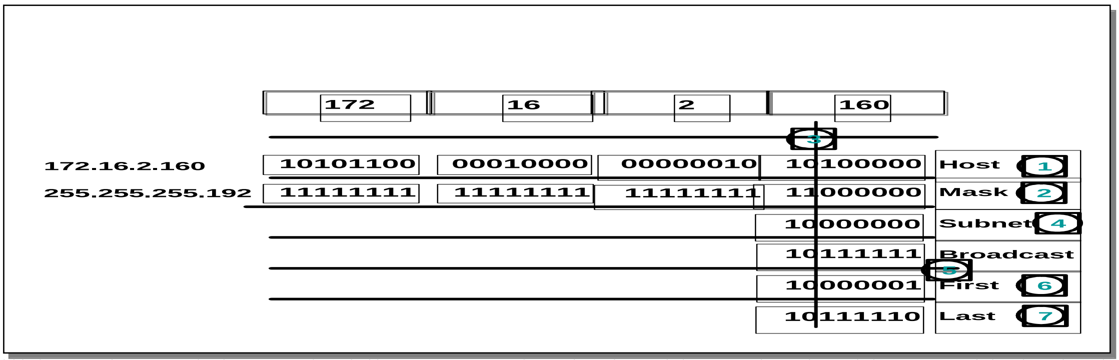
fill in ones beyond the vertical line for the broadcast address

Addressing Summary Example



fill in 0s beyond the vertical line except for the last bit. Make that bit a 1. This is the first usable host address.

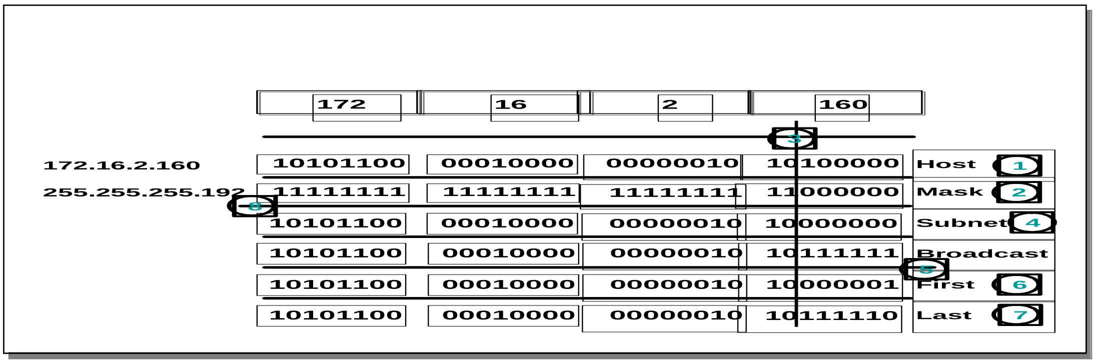
Addressing Summary Example



	172	16	2	160		
				3		
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
				10000000	Subnet	4
				10111111	Broadcast	5
				10000001	First	6
				10111110	Last	7

fill in 1s beyond the vertical line except for the last bit. Make that bit a 0. This is the last usable host address.

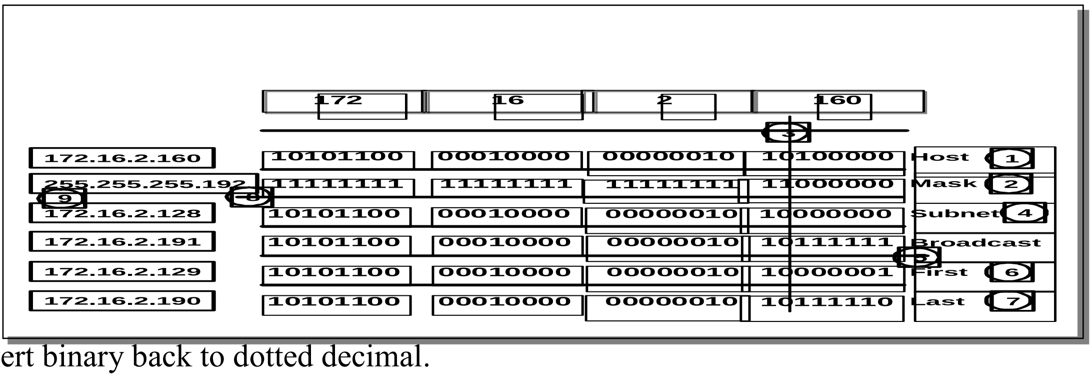
Addressing Summary Example



	172	16	2	160		
				3		
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
8	10101100	00010000	00000010	10000000	Subnet	4
	10101100	00010000	00000010	10111111	Broadcast	5
	10101100	00010000	00000010	10000001	First	6
	10101100	00010000	00000010	10111110	Last	7

copy the binary network and subnetwork address from the top row into the lower rows .

Addressing Summary Example

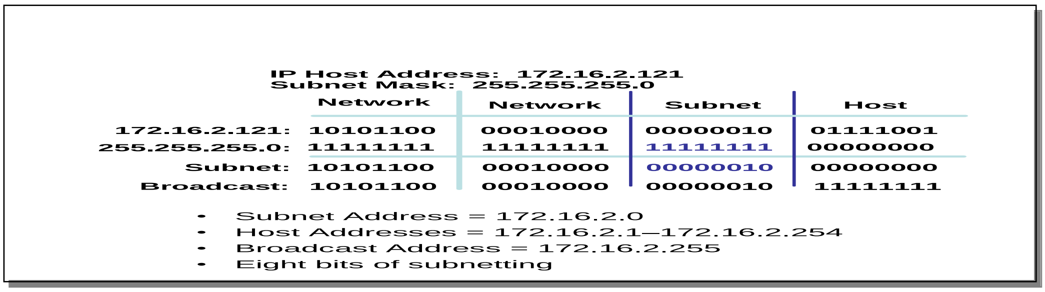


	172	16	2	160		
				3		
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
172.16.2.128	10101100	00010000	00000010	10000000	Subnet	4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast	5
172.16.2.129	10101100	00010000	00000010	10000001	First	6
172.16.2.190	10101100	00010000	00000010	10111110	Last	7

9 8

convert binary back to dotted decimal.

Class B Subnet Example



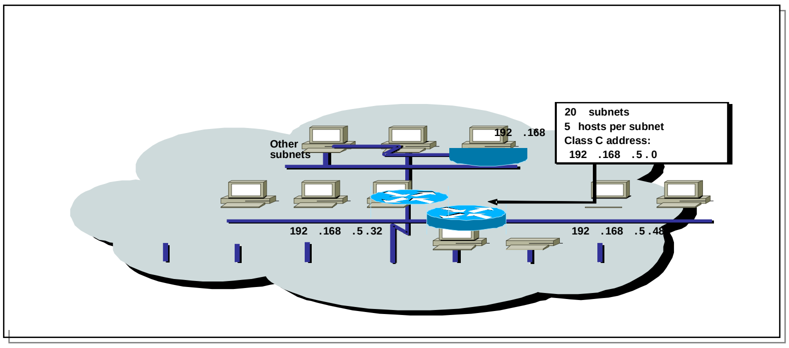
IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subnet:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

- Subnet Address = 172.16.2.0
- Host Addresses = 172.16.2.1–172.16.2.254
- Broadcast Address = 172.16.2.255
- Eight bits of subnetting

This figure shows an example of a Class B network with a subnet

Class B Subnet Planning



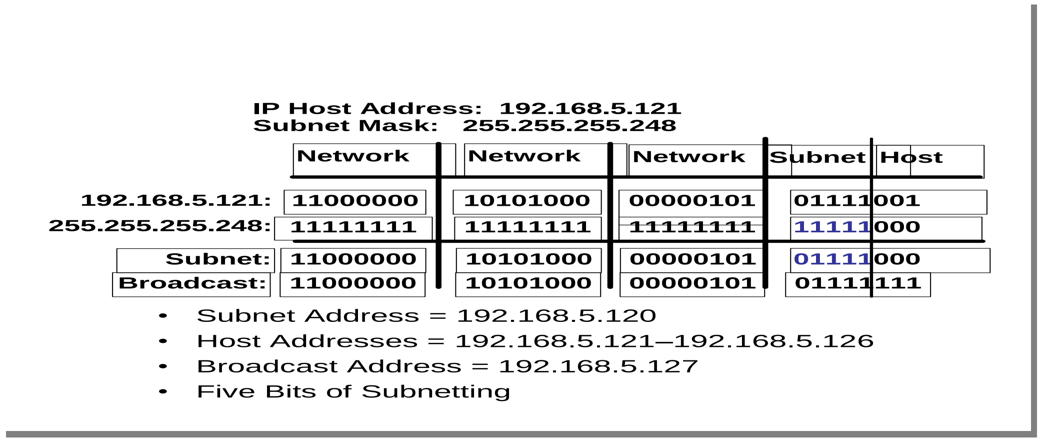
What if this were a Class B address? How many bits would we have for subnetting then? Where do you want to draw the line now؟

Alternatives to review: Creating the subnet at the octet boundary is easier to work with—more host bits and more subnet bits.

Explain that the decision is really a guess on how you think your network will grow—will it have more subnets or more hosts؟

RFC 1219 Mirroring: Mirroring hedges the subnetting decision by buying time. Do not use mirroring if you intend to use route summarization or variable-length subnet masking (VLSM); they are incompatible with mirroring.

Class C Subnet Planning Example



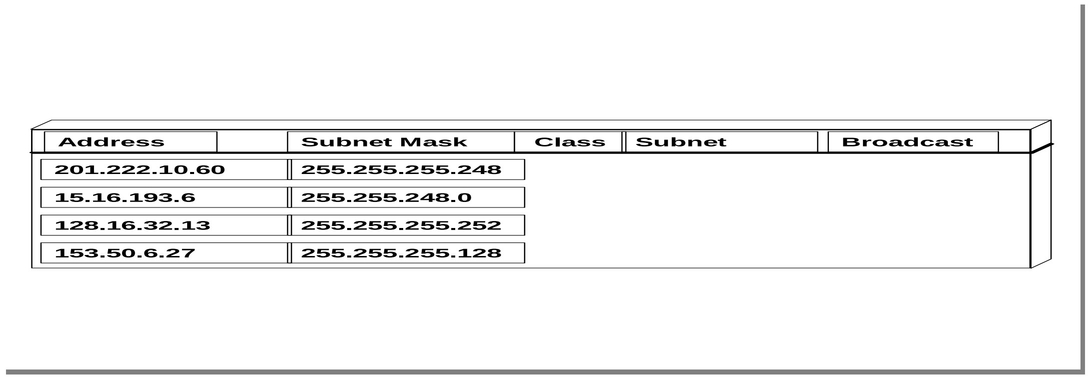
IP Host Address: 192.168.5.121
Subnet Mask: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111	001
255.255.255.248:	11111111	11111111	11111111	11111	000
Subnet:	11000000	10101000	00000101	01111	000
Broadcast:	11000000	10101000	00000101	01111	111

- Subnet Address = 192.168.5.120
- Host Addresses = 192.168.5.121–192.168.5.126
- Broadcast Address = 192.168.5.127
- Five Bits of Subnetting

Contrast the Class C network subnet mask with the previous Class B example.

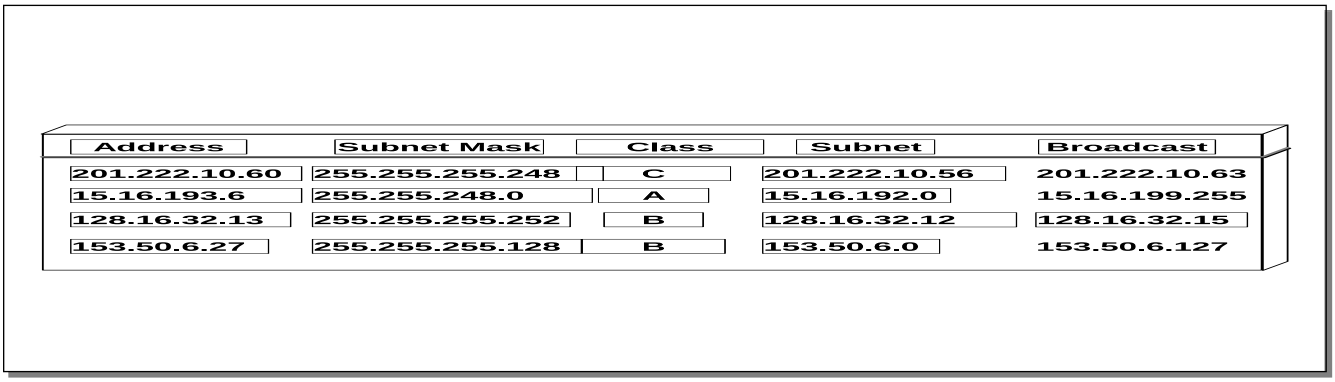
Broadcast Addresses Exercise



Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248			
15.16.193.6	255.255.248.0			
128.16.32.13	255.255.255.252			
153.50.6.27	255.255.255.128			

Have the students calculate the subnet numbers and the broadcast address for each subnet from the given IP addresses and subnet masks.

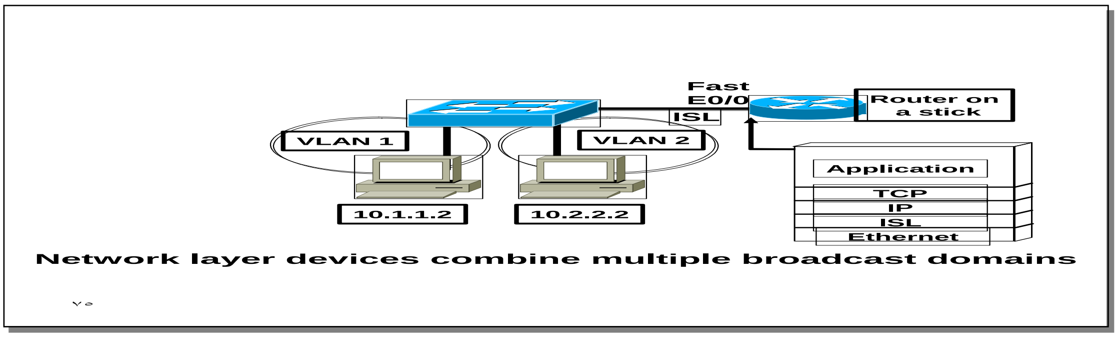
Broadcast Addresses Exercise Answers



Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248	C	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	A	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	B	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	B	153.50.6.0	153.50.6.127

answers to the exercise are given in the figure.

VLAN to VLAN Overview

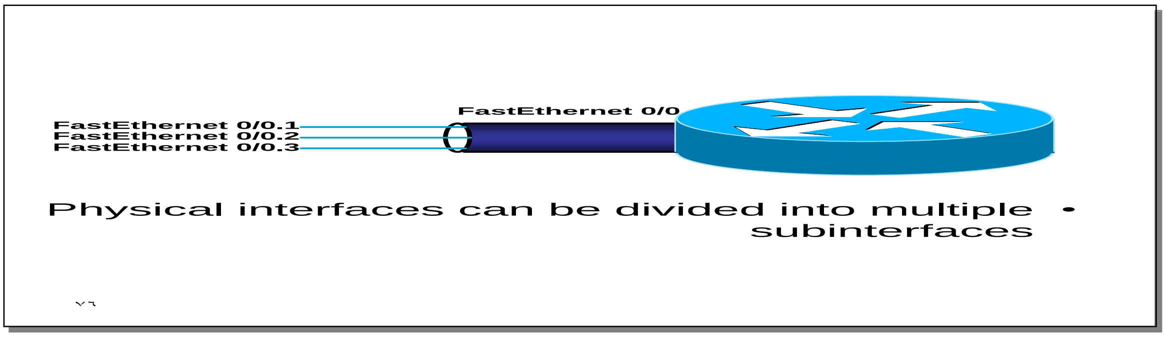


Network layer devices combine multiple broadcast domains

The VLANs are on different networks. Without a network layer device the could not communicate.

Review the protocols operating at each of the OSI layers

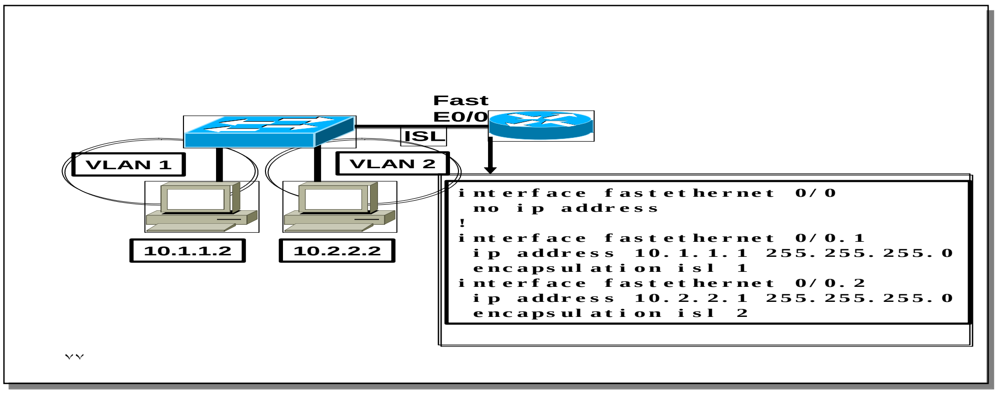
Dividing a Physical Interface into Subinterfaces



- Physical interfaces can be divided into multiple subinterfaces

At this point, it is important for students t understand that if they want to connect multiple VLANs, they need a separate connection for each VLAN. This can be accomplished by establishing a physical connection for each VLAN that will interconnect with other VLANs or by splitting a trunk into multiple, logical subinterfaces.

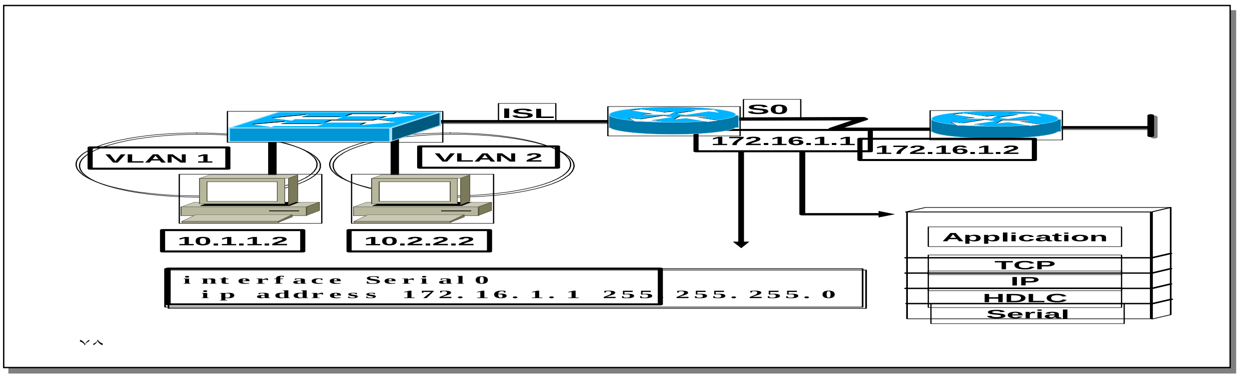
Routing Between VLANs



```
interface fastethernet 0/0
 no ip address
!
interface fastethernet 0/0.1
 ip address 10.1.1.1 255.255.255.0
 encapsulation isl 1
interface fastethernet 0/0.2
 ip address 10.2.2.1 255.255.255.0
 encapsulation isl 2
```

Highlight the two different networks, 10.1.1.0 and 10.2.2.0, interconnecting.

Routing Between WANS



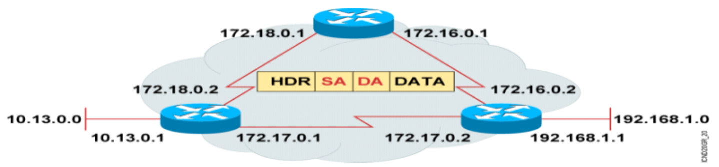
```
interface Serial0
 ip address 172.16.1.1 255 255.255.0
```

This figure shows that the same principals apply when interconnecting WANs.

Note: HDLC is used in this example because it is on by default. Students just need to know that it is Cisco’s default serial layer 2 encapsulation.

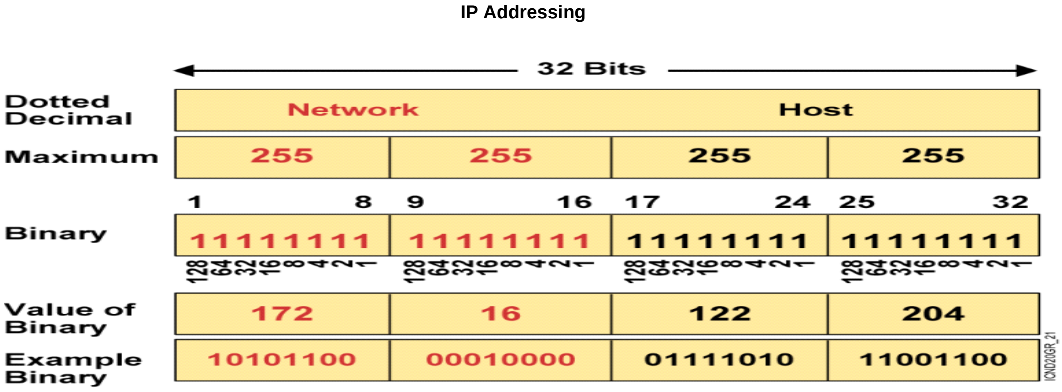
Introducing IP Addresses

Introducing IP Addresses



Unique addressing allows communication between end stations.
Path choice is based on destination address.

Stations with internetwork access must have unique addresses.



IP Addressing

32 Bits

Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 8	9 16	17 24	25 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Value of Binary	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

an example of dotted decimal format and binary are displayed.

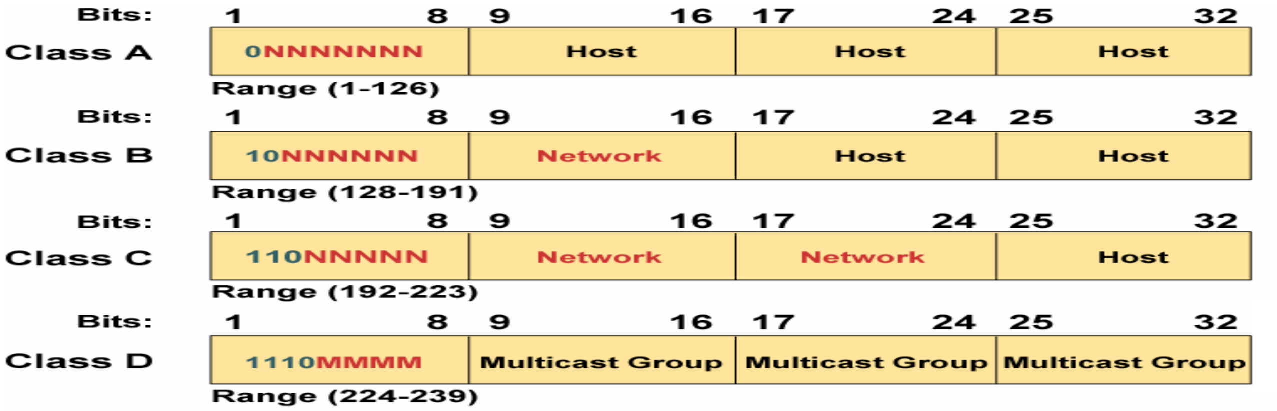
IP address format is dotted decimal. Dotted decimal makes it easy to work with IP addresses. However, in this course we will work with the addresses on the bit level, so we will convert these addresses into binary, make changes to them, and convert them back.

The central authority for addresses is the Internet Assigned Numbers Authority (IANA.(

Note: This most common form of addressing reflects the widely used IP version 4. Faced with the problem of depleting available addresses, Internet Engineering Task Force (IETF) work is under way for a backward-compatible next generation of IP (IPng, also called IP 6 .(

IP 6 will offer expanded routing and addressing capabilities with 128-bit addresses rather than the 32-bit addressing shown on the graphic. Addresses from both IP versions will coexist. Initial occurrences will probably be at locations with address translator software and firewalls

IP Address Classes



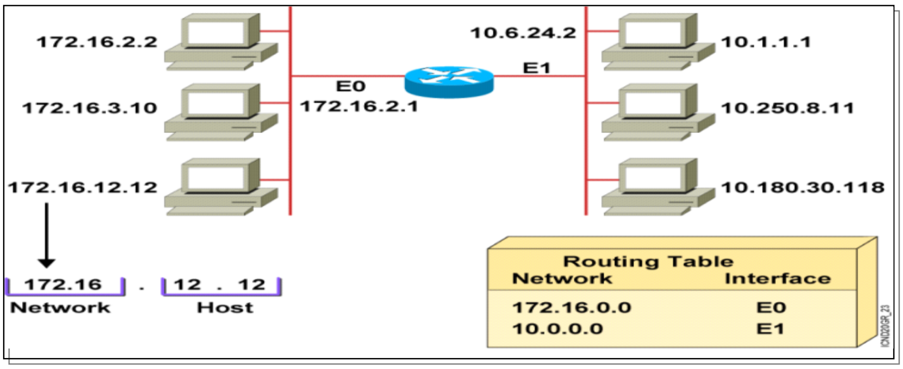
Bits:	1 8	9 16	17 24	25 32
Class A	0NNNNNNN	Host	Host	Host
	Range (1-126)			
Bits:	1 8	9 16	17 24	25 32
Class B	10NNNNNN	Network	Host	Host
	Range (128-191)			
Bits:	1 8	9 16	17 24	25 32
Class C	110NNNNN	Network	Network	Host
	Range (192-223)			
Bits:	1 8	9 16	17 24	25 32
Class D	1110MMMM	Multicast Group	Multicast Group	Multicast Group
	Range (224-239)			

High light the fixed values that start each class address.

The first octet rule states that when an address falls into a specified range, it belongs to a certain class. Students should soon be able to recognize the address class of any IP address on sight.

Note: If time or interest permits, you can use the initial bit patterns in the first octet and show how a class of IP network derives the range of network numbers for that IP address class.

Host Addresses



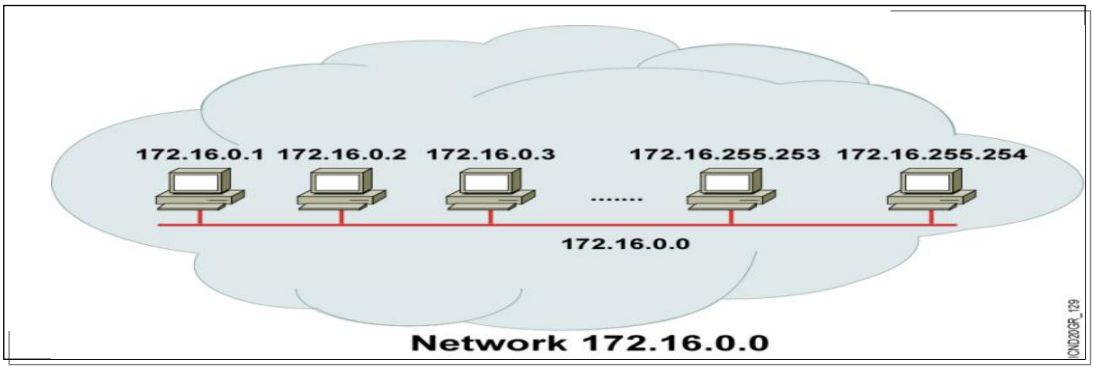
Routing Table

Network	Interface
172.16.0.0	E0
10.0.0.0	E1

In the example, 172.16.0.0 and 10.0.0.0 refer to the wires at each end of the router .

Explain how the routing table is used. Entries in the routing table refer to the network only. The router does not know the location of hosts; it knows the location of networks.

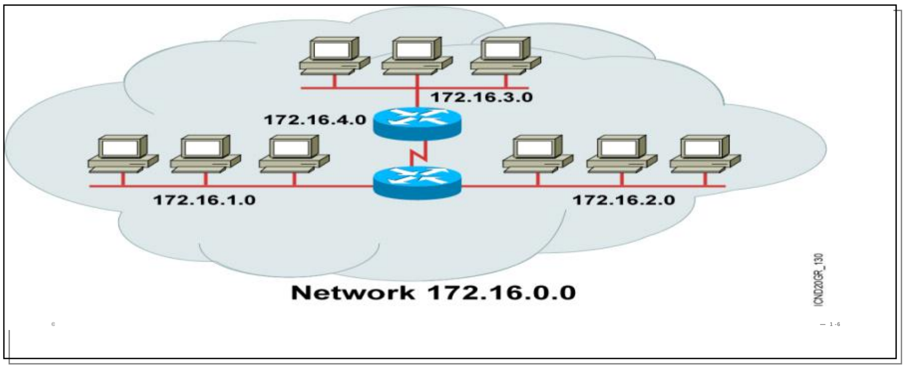
Addressing Without Subnets



Without subnets, use of network addressing space is inefficient .

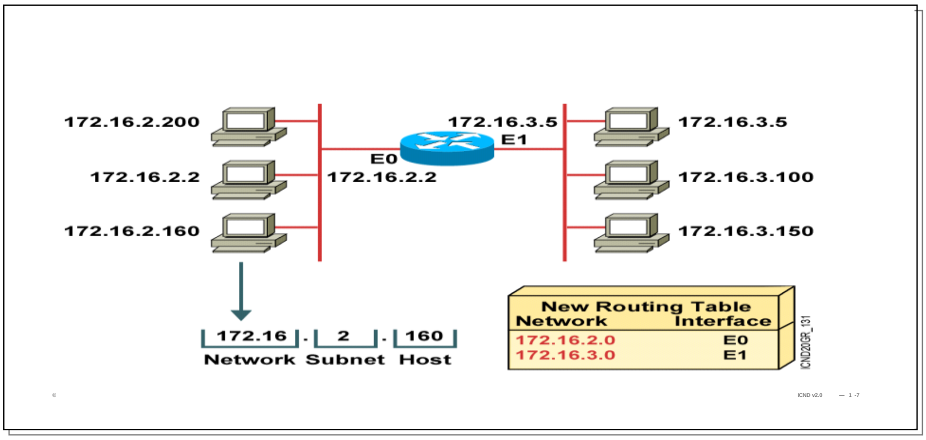
The Class B network is like a highway with no exits—there is no place to exit, so all of the traffic is in one line.

Addressing with Subnets



The host bits of an IP address can be subdivided into a subnetwork section and a host section. The subnetwork section in this example is the full third octet.
Point out the difference in the addressing between the previous slide and this slide.
A subnetted address space is like a highway with exits.
A network device uses a subnet mask to determine what part of the IP address is used for the network, the subnet, and the device ID .
A subnet mask is a 32-bit value containing a number of one bits for the network and subnet ID, and a number of zero bits for the host ID .
Given its own IP address and subnet mask, a device can determine if an IP packet is destined for 1) a device on its own subnet, 2) a device on a different subnet on its own network, or 3) a device on a different network .
A device can determine what class of address the device has been assigned from its own IP address. The subnet mask then tells the device where the boundary is between the subnet ID and the host ID

Subnet Addressing

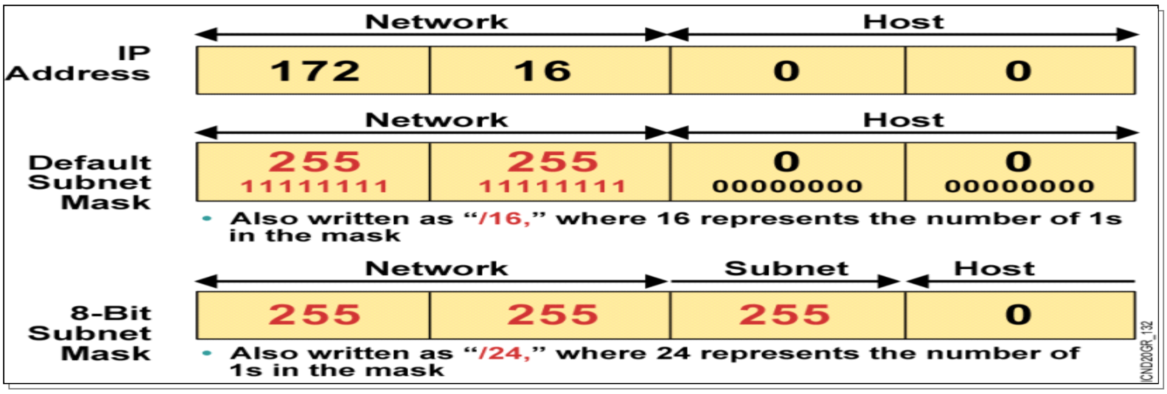


New Routing Table

Network	Interface
172.16.2.0	E0
172.16.3.0	E1

By turning on more bits in the mask, we reserve some bits as network information and can use these bits to describe subnetworks .
Describe how the router makes use of this technique. Point out that there is more information in the routing table now.

Subnet Mask



	Network		Host	
IP Address	172	16	0	0
	Network		Host	
Default Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000
	Network		Subnet	Host
8-Bit Subnet Mask	255	255	255	0

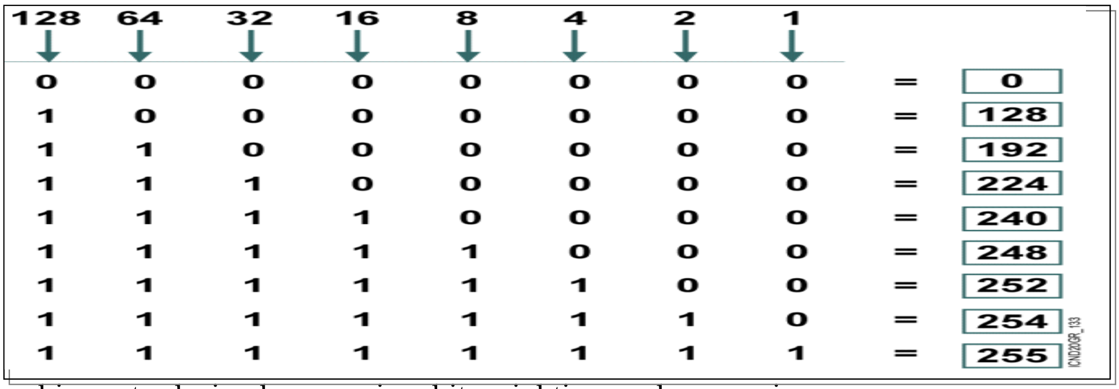
- Also written as "/16," where 16 represents the number of 1s in the mask
- Also written as "/24," where 24 represents the number of 1s in the mask

Turn on more bits to represent subnets.Compare the default or standard subnet mask with the subnet mask in the slide.The following are the rules for IP addressing:
An address is 32 bits, divided into three components :First octet rule bitsNetwork bits (path selection bits(Node bitsThe first octet rule states that the most significant bit pattern in the first octet determines the class of the address.Path selection bits cannot be all ones or zeros.Certain addresses are reserved. RFC 1918 defines some of those.Prefix or mask one bits are path selection significant; zero bits are

host bits and therefore not significant.Use the logical AND to combine the address and mask bits to get the subnet address.

The maximum number of available subnets equals 2 prefix bits - 2; the maximum number of available hosts equals 2 32- prefix bits - 2.

Decimal Equivalents of Bit Patterns



128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	=	0
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

ICND20GR_133

Review binary-to-decimal conversion, bit weighting, and conversion.

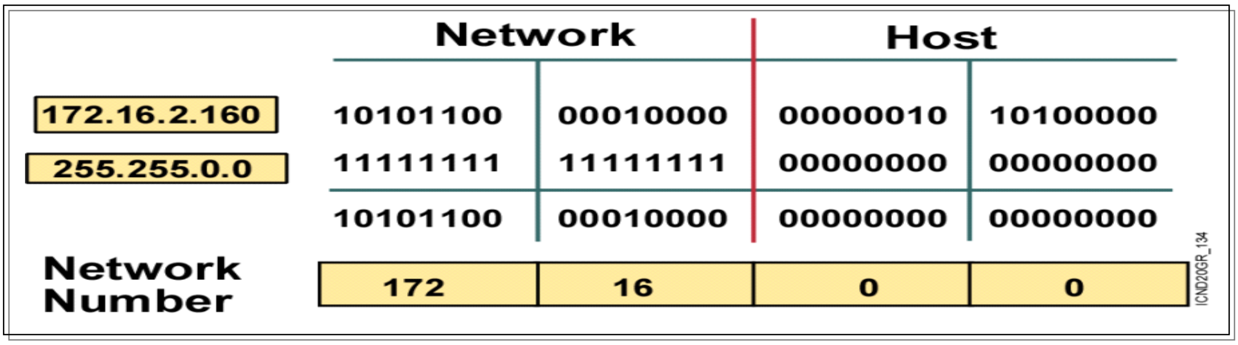
Explain the logical AND.

One possible explanation of the logical AND follows. We will need to be able to perform a logical AND on the binary numbers. Just take two binary numbers and place one above the other. The ones in the bottom are like a pipe—the number above it just drops through. The zeros are like a clogged pipe, so nothing comes out in the answer.

Presenting a truth table will help some students understand. You might need to give more than one explanation.

Note: You might want to hand out a binary-to-decimal conversion sheet if you have not already done so. We have not included one in the lab section. It is more useful to have one that is on a separate page from the labs.

Subnet Mask Without Subnets



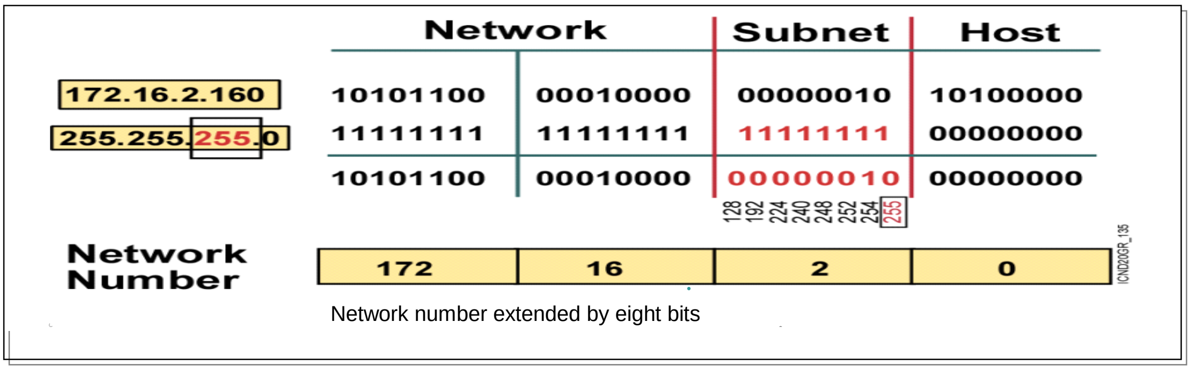
	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

ICND20GR_134

Explain how masking works at the bit level. Zero bits mask host information.

Note: This is an easy place to lose students. At this point, they need to learn several abstract mathematical concepts before we can show them how to lay out an IP-addressed network. To the novice, these techniques may seem unrelated, making the presentation confusing. To a more experienced audience, these techniques will be familiar.

Subnet Mask with Subnets



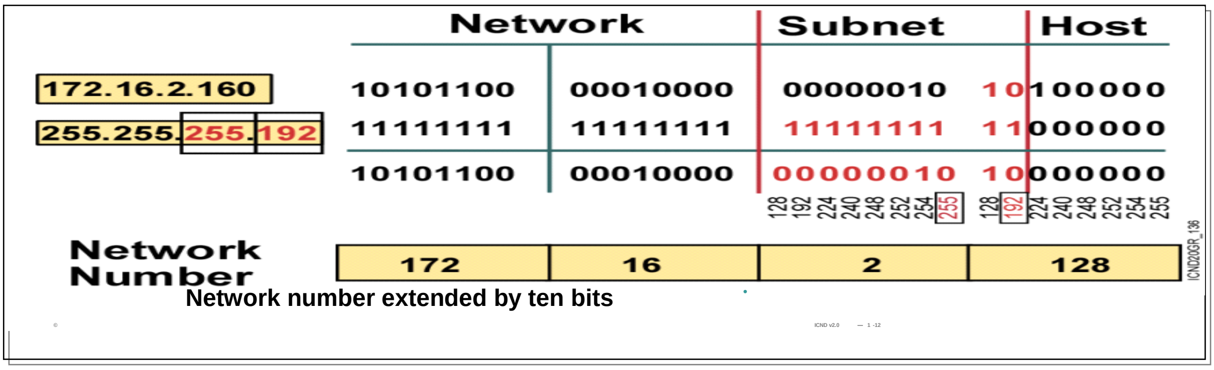
	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
			128 192 224 240 248 252 254 255	
Network Number	172	16	2	0

Network number extended by eight bits

ICND20GR_135

This example makes a Class B address space look like a collection of Class C address spaces.
Now the logical AND allows us to extract the subnet number as well as the assigned network number.
An exercise follows that tests the students' understanding of subnet masks.

Subnet Mask with Subnets (Cont.)



	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
			128 192 224 240 248 252 254 255	128 192 224 240 248 252 254 255
Network Number	172	16	2	128

Network number extended by ten bits

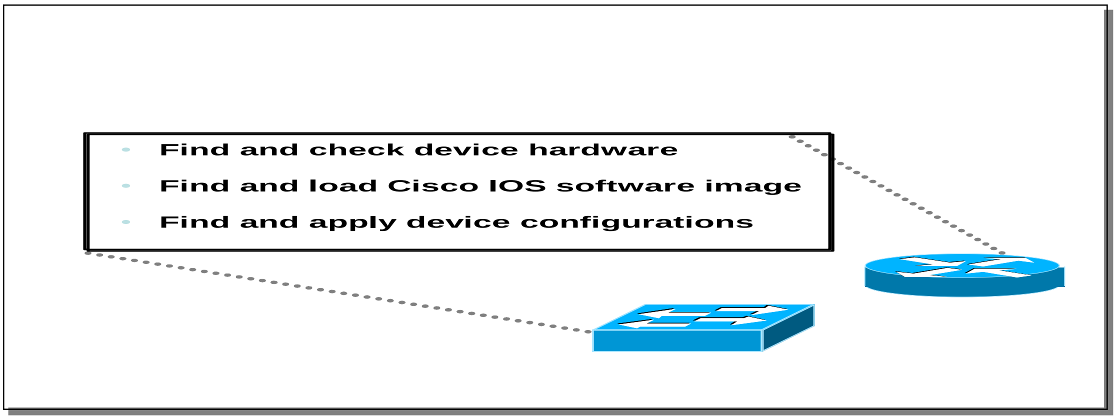
ICND20GR_136

This example is different from the previous example in that the the subnet and host are divided within an octet.
Transition: An exercise follows that tests the students' understanding of subnet masks.

Network Device Configuration

Configuration sets up the device with:
- Network policy of the functions required
-Protocol addressing and parameter settings
- Options for administration and management
Catalyst switch memory has initial configuration
with default settings
Cisco router will prompt for initial configuration if
there is no configuration in memory

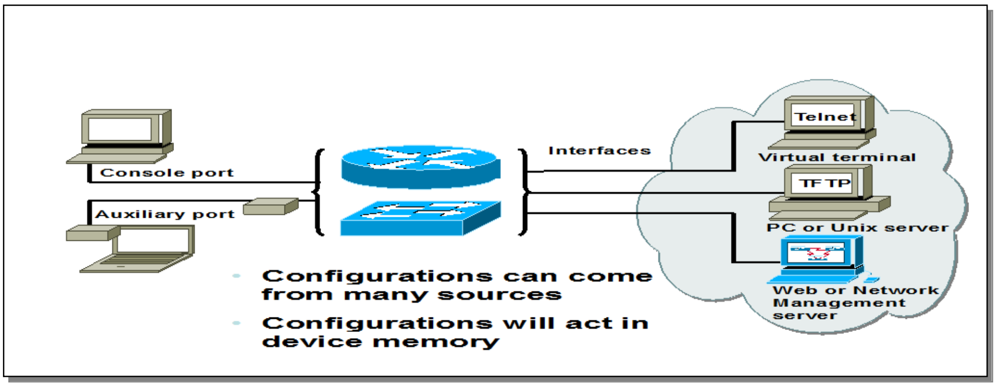
An Overview of Cisco Device Startup



- Find and check device hardware
- Find and load Cisco IOS software image
- Find and apply device configurations

Paraphrase or restate the three points and make sure your students follow the description. This description is necessary to keep a common perspective of what is occurring on first the switch and then the router; these three steps should be an anchor to return to as needed .
This overview of what happens with Cisco network device start up transitions to the next topic: Where are the sources for configuration software ؟

External Configuration Sources


Console port
Auxiliary port
Interfaces
Telnet
Virtual terminal
TFTP
PC or Unix server
Web or Network Management server
Configurations can come from many sources
Configurations will act in device memory

The network device can be configured from several locations. After you create the initial configuration, you can configure the ports or interfaces to enable configuration over virtual terminals ports (VTY.(
Both router and switch support telnet access as a virtual terminal .
The router by default, supports virtual terminals 0 through 4. That means that router can be accessed for configuration purposes from the console port, the auxiliary port, and five VTY lines at the same time—up to seven people can configure the router at once .
You should caution students about the above point and inform them that security should be strictly observed through password protection to avoid unauthorized access of the configuration files .
Another component important to configuration in the network is a TFTP server.
The TFTP server can be a UNIX or PC workstation that acts as a central depository for files .
You can keep configuration files on the TFTP server and then download them to the device .
You can also configure the from a network management station running network management software such as CWSI, CiscoWorks or HP OpenView. Before you can access or change the configuration from a virtual terminal, TFTP server, or network management station, you must have the device configured to support IP traffic .

Cisco IOS User Interface Fundamentals

*Uses a command line interface
*Operations vary on different internetworking devices
*Type or paste entries in the console command modes
*Enter key instructs device to parse and execute the command
*Two primary EXEC modes are user mode and privileged mode
*Command modes have distinctive prompts

Cisco IOS Software EXEC

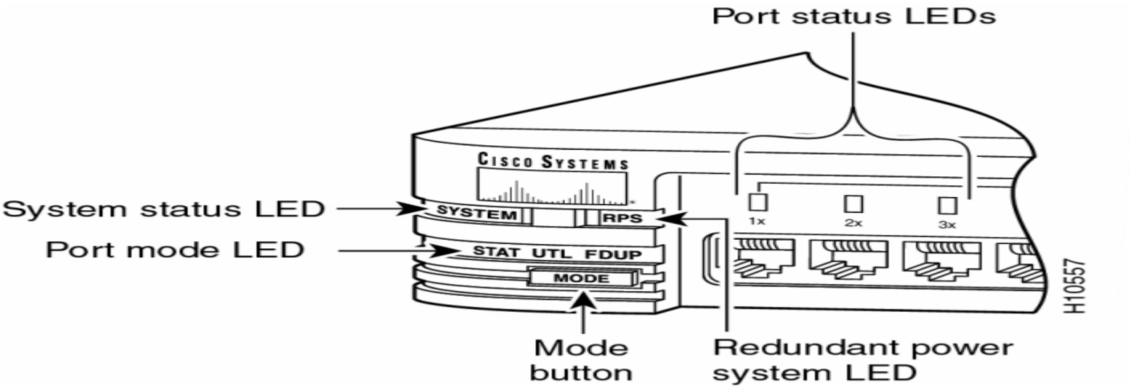
There are two main EXEC modes for entering commands.
First mode:
User Mode
*Limited examination of switch or router
*Command Prompt is hostname>

The Cisco IOS Software EXEC (cont.)

Second mode (and most commonly used):
Privileged (or enabled) Mode

*Detailed examination of switch or router
*Enables configuration and debugging
*Prerequisite for other configuration modes
*Command prompts on the device
hostname#
Initial Start up of the Catalyst Switch
*System startup routines initiate switch software
*Initial startup uses default configuration parameters
1. Before you start the switch, verify the cabling and console connection
2. Attach the power cable plug to the switch power supply socket
3. Observe the boot sequence
*LEDs on the switch chassis
*Cisco IOS software output text

Checking Switch LED Indicators

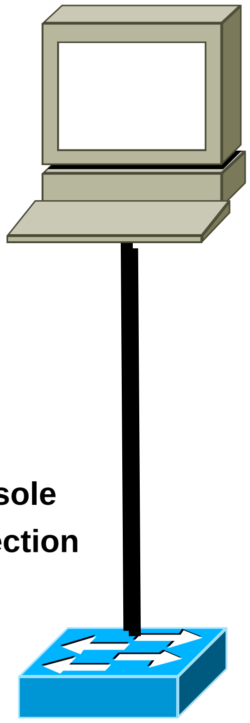


Port LEDs during Switch POST

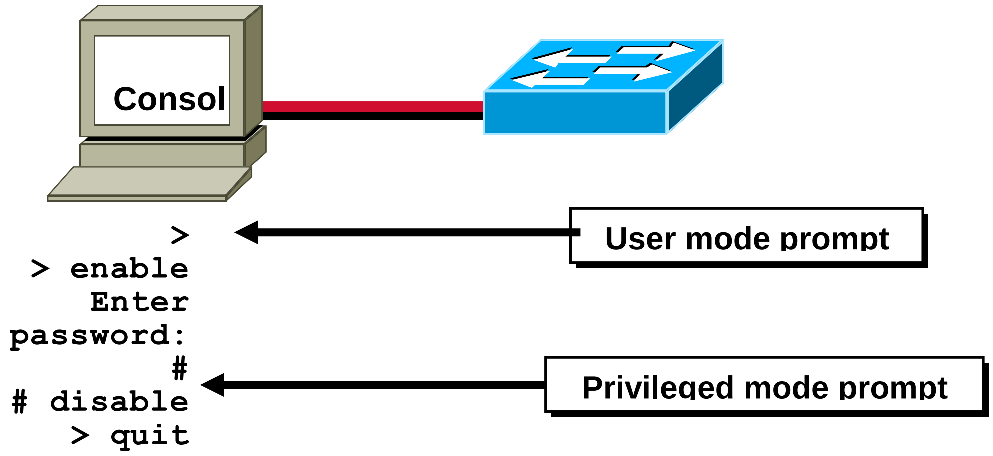
1. At the start, all port LEDs are green.
2. Each LED turns off after its test completes.
3. If a test fails, its LED turns amber.
4. System LED turns amber if any test fails.
5. If no test fails, POST completes.
6. On POST completion, LEDs blink
  then turn off.

Initial Bootup Output from the Switch

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address:       00-50-BD-73-E2-C0

PCA Number:             73-3121-01
PCA Serial Number:      FAA0252A0QX
Model Number:           WS-C1924-EN
System Serial Number:   FAA0304S0U3
Power Supply S/N:       PHI025101F3
-------------------------------------------------

1 user(s) now active on Management Console.

        User Interface Menu

     [M] Menus
     [K] Command Line
     [I] IP Configuration

Enter Selection:
```



Logging into the Switch and Entering the Enable Password



```
        >
> enable
    Enter
password:
        #
# disable
   > quit
```

Switch Command Line Help Facilities

Context-Sensitive Help

Provides a list of commands and the arguments associated with a specific command.

Console Error Messages

Identify problems with switch commands incorrectly entered so that you can alter or correct them.

Command History Buffer

Allows recall of long or complex commands or entries for reentry, review, or correction.

Showing Switch Initial Startup Status

```
Switch#show version
```

```
Switch#show runningconfig
```

```
Switch#show interfaces
```

Display operational status of switch components

Switch show version Command

```
wg_sw_c# show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.01     written from 171.068.229.225
Copyright (c) Cisco Systems, Inc.  1993-1998
wg_sw_c uptime is 15day(s) 21hour(s) 53minute(s) 11second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
```

```
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-BD-73-E2-C0
```

Switch show running-configuration Command

Catalyst 1924

```
wg_sw_c#show run

Building configuration...
Current configuration:
!
hostname "wg_sw_c"
!
ip address 10.1.1.33
255.255.255.0
ip default-gateway 10.3.3.3
!
interface Ethernet 0/1
<text omitted>
interface Ethernet 0/24
!
Interface Ethernet 0/25
!
interface FastEthernet 0/26
!
interface FastEthernet 0/27
```

Catalyst 1912

```
wg_sw_c#show run

Building configuration...
Current configuration:
!
hostname "wg_sw_c"
!
ip address 10.1.1.33 255.255.255.0
ip default-gateway 10.3.3.3
!
interface Ethernet 0/1
<text omitted>
interface Ethernet 0/12
!
Interface Ethernet 0/25
!
interface FastEthernet 0/26
!
interface FastEthernet 0/27
```

This page shows the format and output of the show running-config on the 1912 and 1924. There is a slide in chapter 6 that covers the port numberings on **the Cat 1912**

Switch show interfaces Command

wg_sw_c#show interfaces ethernet 0/1

```
Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0050.BD73.E2C1
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State:  Forwarding     Forward Transitions:  1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description:
Duplex setting: Half duplex
Back pressure: Disabled
--More--
```

Showing the Switch IP Address

wg_sw_a#show ip

```
IP Address: 10.5.5.11
Subnet Mask: 255.255.255.0
Default Gateway: 10.5.5.3
Management VLAN:  1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port :  80
RIP : Enabled
wg_sw_a#
```

Configuring the SwitchConfiguration Modes:

*Global Configuration Mode
-wg_sw_a# conf term
-wg_sw_a(config)#
*Interface Configuration Mode
-wg_sw_a(config)# interface e0/1
-wg_sw_a(config-if)#

Configuring Switch Identification

Switch Name
(config)#hostname **MONA**
MONA(config)#

Configuring the Switch
Configuration Modes:
*Global Configuration Mode
-MONA# conf term
-MONA(config)#
*Interface Configuration Mode
MONA(config)# interface e0/1
MONA(config-if)#

*Configuring Switch Identification

Switch Name
(config)#hostname MONA
MONA(config)#
Sets local identity for the switch

*Configure the Switch IP Address

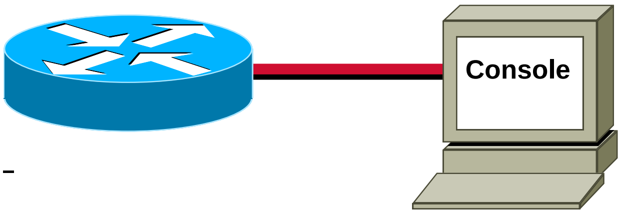
MONA(config)# ip address {ip address} {mask}
MONA(config)#ip address 10.5.5.11 255.255.255.0

* Initial Start Up of the Cisco Router

*System startup routines initiate router software
*Router falls back to startup alternatives if needed

1. Before you start the router, verify the power, cabling, and console connection
2. Push the power switch to on
3. Observe the boot sequence
   Cisco IOS software output text on the console

* BootUp Output from the Router



```
    --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[ ]'.
```

Setup mode

```
MONA con0 is now available


Press RETURN to get started.
```

User-mode

Setup: The Initial Configuration Dialog

MONA#setup

```
        --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: n
```

Setup Interface Summary

```
First, would you like to see the current interface summary? [yes]:
Interface        IP-Address     OK? Method Status              Protocol
BRI0             unassigned     YES unset  administratively down down
BRI0:1           unassigned     YES unset  administratively down down
BRI0:2           unassigned     YES unset  administratively down down
Ethernet0        unassigned     YES unset  administratively down down
Serial0          unassigned     YES unset  administratively down down
```

- **Interfaces found during startup**

Setup Global Parameters

```
Configuring global parameters:
 Enter host name [Router]:MONA
 The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: cisco
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: sanfran
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: sanjose
  Configure SNMP Network Management? [no]:
```

Setup Global Parameters (cont.)

```
  Configure LAT? [yes]: n
  Configure AppleTalk? [no]:
  Configure DECnet? [no]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]: n
    Configure RIP routing? [no]:
  Configure CLNS? [no]:
  Configure IPX? [no]:
  Configure Vines? [no]:
  Configure XNS? [no]:
  Configure Apollo? [no]:
```

Setup Interface Parameters

```
BRI interface needs isdn switch-type to be configured
  Valid switch types are :
              [0]  none..........Only if you don't want to configure BRI.
              [1]  basic-1tr6....1TR6 switch type for Germany
              [2]  basic-5ess....AT&T 5ESS switch type for the US/Canada
              [3]  basic-dms100..Northern DMS-100 switch type for US/Canada
              [4]  basic-net3....NET3 switch type for UK and Europe
              [5]  basic-ni......National ISDN switch type
              [6]  basic-ts013...TS013 switch type for Australia
              [7]  ntt...........NTT switch type for Japan
              [8]  vn3...........VN3 and VN4 switch types for France
  Choose ISDN BRI Switch Type [2]:
Configuring interface parameters:
Do you want to configure BRI0 (BRI d-channel) interface? [no]:
Do you want to configure Ethernet0  interface? [no]: y
  Configure IP on this interface? [no]: y
    IP address for this interface: 10.1.1.33
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 10.0.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial0  interface? [no]:
Setup Global Parameters (cont.)
  Configure LAT? [yes]: n
  Configure AppleTalk? [no]:
  Configure DECnet? [no]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]: n
    Configure RIP routing? [no]:
  Configure CLNS? [no]:
  Configure IPX? [no]:
```

```
 Configure Vines? [no]:
 Configure XNS? [no]:
 Configure Apollo? [no]:
```

Setup Interface Parameters

```
BRI interface needs isdn switch-type to be configured
 Valid switch types are :
            [0]  none..........Only if you don't want to configure BRI.
            [1]  basic-1tr6....1TR6 switch type for Germany
            [2]  basic-5ess....AT&T 5ESS switch type for the US/Canada
            [3]  basic-dms100..Northern DMS-100 switch type for US/Canada
            [4]  basic-net3....NET3 switch type for UK and Europe
            [5]  basic-ni......National ISDN switch type
            [6]  basic-ts013...TS013 switch type for Australia
            [7]  ntt...........NTT switch type for Japan
            [8]  vn3...........VN3 and VN4 switch types for France
 Choose ISDN BRI Switch Type [2]:
```

Configuring interface parameters:

```
Do you want to configure BRI0 (BRI d-channel) interface? [no]:
Do you want to configure Ethernet0  interface? [no]: y
 Configure IP on this interface? [no]: y
 IP address for this interface: 10.1.1.33
 Subnet mask for this interface [255.0.0.0] : 255.255.255.0
  Class A network is 10.0.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial0  interface? [no]:
```

Setup Script Review and Use

```
 following configuration command script was created:

hostname Router
 enable secret 5 $1$/CCk$4r7zDwDNeqkxFO.kJxC3G0
  enable password sanfran
     line vty 0 4
      password sanjose
     no snmp-server

       no appletalk routing
        no decnet routing
      ip routing
        no clns routing
       no ipx routing
       no vines routing
          no xns routing
      no apollo routing
    isdn switch-type  basic-5ess
```

```
  interface BRI0
  shutdown
 no ip address

 interface Ethernet0
   no shutdown
    ip address 10.1.1.31 255.255.255.0
  no mop enabled

 interface Serial0
   shutdown
    no ip address
  <text omitted>

[0] Go to the IOS command prompt without saving this config.
  [1] Return back to the setup without saving this config.
       [2] Save this configuration to nvram and exit.

          Enter your selection [2]:
```

Logging into the Router

```
MONA  con0 is now available
Press RETURN to get started.
MONA>
MONA>enable
MONA#
MONA#disable
MONA>
MONA>logout
```

Router User Mode Command List

MONA>?

Exec commands:

```
  access-enable    Create a temporary Access-List entry
  atmsig           Execute Atm Signalling Commands
  cd               Change current device
  clear            Reset functions
  connect          Open a terminal connection
  dir              List files on given device
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lat              Open a lat connection
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
-- More --
```

You can abbreviate a command to the fewest characters that make a unique character string

Router Privileged Mode Command List

MONA#?

```
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
-- More --
```

Router Command Line Help Facilities

Context-Sensitive Help

Provides a list of commands and the arguments associated with a specific command.

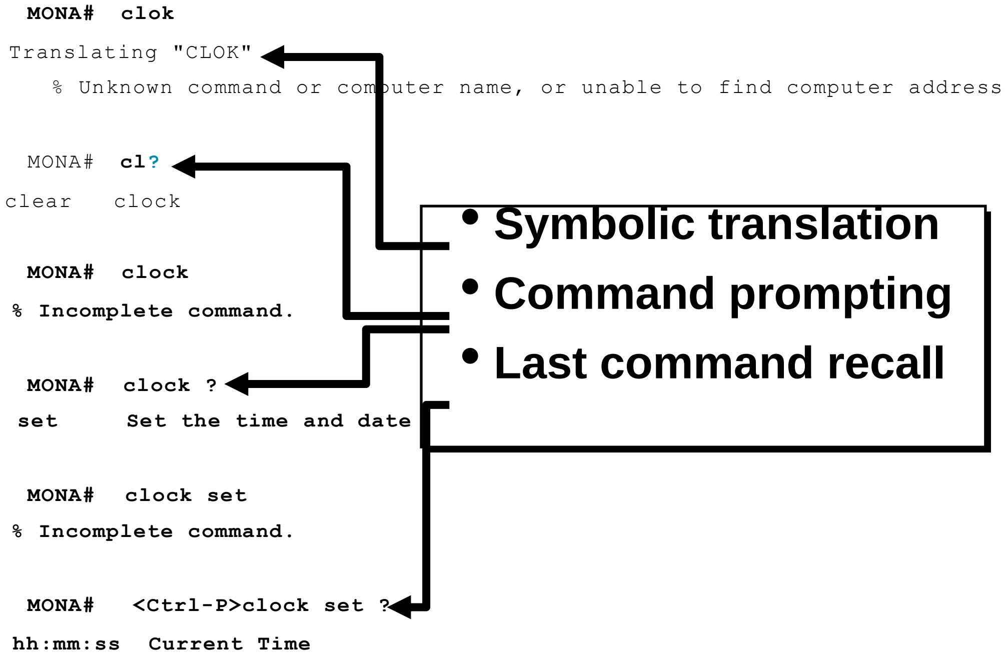
Console Error Messages

Identify problems with router commands incorrectly entered so that you can alter or correct them.

Command History Buffer

Allows recall of long or complex commands or entries for reentry, review, or correction.

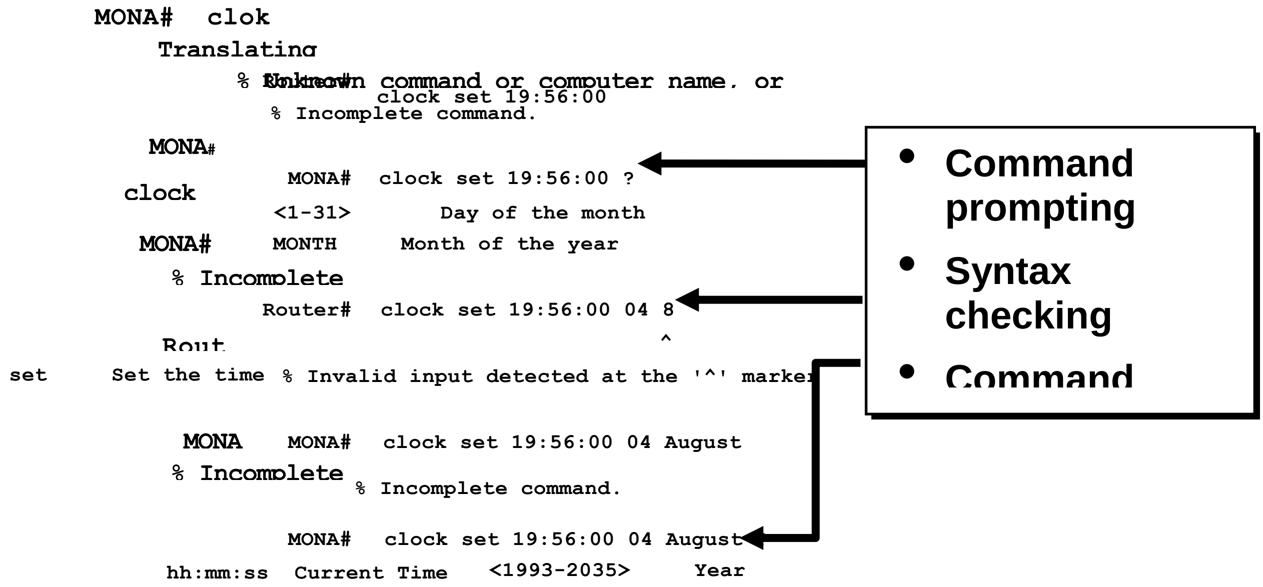
Router Context-Sensitive Help



```
  MONA#  clok
Translating "CLOK"
   % Unknown command or computer name, or unable to find computer address

  MONA#  cl?
clear   clock

  MONA#  clock
% Incomplete command.

  MONA#  clock ?
set     Set the time and date

  MONA#  clock set
% Incomplete command.

  MONA#  <Ctrl-P>clock set ?
hh:mm:ss  Current Time
```

- Symbolic translation
- Command prompting
- Last command recall

Router Context-Sensitive Help (cont.)



```
    MONA#  clok
        Translating
              % Unknown command or computer name, or
                     clock set 19:56:00
                 % Incomplete command.
      MONA#
                  MONA#  clock set 19:56:00 ?
    clock
                 <1-31>       Day of the month
     MONA#       MONTH      Month of the year
        % Incomplete
                Router#  clock set 19:56:00 04 8
         Rout                                  ^
set     Set the time  % Invalid input detected at the '^' marker

           MONA    MONA#  clock set 19:56:00 04 August
        % Incomplete  % Incomplete command.

                  MONA#  clock set 19:56:00 04 August
        hh:mm:ss  Current Time   <1993-2035>     Year
```

- Command prompting
- Syntax checking
- Command

Using Enhanced Editing Commands

```
MONA>Shape the future of internetworking by creating unpreced
```

Shape the future of internetworking by creating unprecedented value for customers, employees, and partners.

Using Enhanced Editing Commands

```
MONA>$ future of internetworking by creating unprecedented op
```

(Automatic scrolling of long lines).

Using Enhanced Editing Commands

```
MONA>Shape the value of internetworking by creating unpreced
```

(Automatic scrolling of long lines).

Ctrl-A (Move to the beginning of the command line.)

Using Enhanced Editing Commands

```
MONA>$ value for customers, employees, and partners.
```

(Automatic scrolling of long lines).

<Ctrl-A>   (Move to the beginning of the command line.)

<Ctrl-E>   (Move to the end of the command line.)

Using Enhanced Editing Commands

```
MONA>$ value for customers, employees, and partners.
```

(Automatic scrolling of long lines).

<Ctrl-A>   (Move to the beginning of the command line.)

<Ctrl-E>   (Move to the end of the command line.)

<Esc-B>   (Move back one word.)

Using Enhanced Editing Commands

```
MONA>$ value for customers, employees, and partners.
```

(Automatic scrolling of long lines).

<Ctrl-A>   (Move to the beginning of the command line.)

<Ctrl-E>   (Move to the end of the command line.)

<Esc-B>   (Move back one word.)

<Ctrl-F> (Move forward one character.)

Using Enhanced Editing Commands

```
MONA>$ value for customers, employees, and partners.
```

(Automatic scrolling of long lines).

<Ctrl-A>   (Move to the beginning of the command line.)

<Ctrl-E>   (Move to the end of the command line.)

<Esc-B>   (Move back one word.)

<Ctrl-F> (Move forward one character.)

<Ctrl-B> (Move back one character.)

Using Enhanced Editing Commands

```
MONA>$ value for customers, employees, and partners.
```

(Automatic scrolling of long lines).

<Ctrl-A>   (Move to the beginning of the command line.)

<Ctrl-E>   (Move to the end of the command line.)

<Esc-B>   (Move back one word.)

<Ctrl-F> (Move forward one character.)

<Ctrl-B> (Move back one character.)

<Esc-F>   (Move forward one word.)

Using Enhanced Editing Commands

MONA>$ value for customers, employees, and partners.
(Automatic scrolling of long lines).
<Ctrl-A> (Move to the beginning of the command line.)
<Ctrl-E> (Move to the end of the command line.)
<Esc-B> (Move back one word.)
<Ctrl-F> (Move forward one character.)
<Ctrl-B> (Move back one character.)
<Esc-F> (Move forward one word.)
<Ctrl-D> (Delete a single character.)
Reviewing Router Command History

Ctrl-P or Up arrow	Last (previous) command recall
Ctrl-N or Down arrow	More recent command recall
MONA> show history	Show command buffer contents
MONA> terminal history size lines	Set session command buffer size

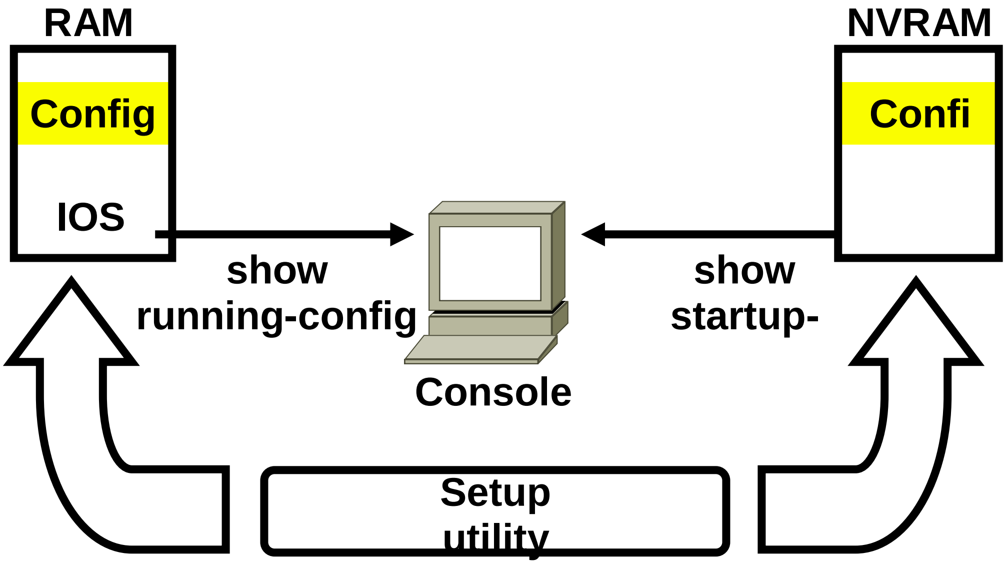
show version Command

MONA#show version

```
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
Image text-base: 0x03050C84, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE(fc1)

wg_ro_a uptime is 20 minutes
System restarted by reload
System image file is "flash:c2500-js-l_120-3.bin"
(output omitted)
--More--
```

```
Configuration register is 0x2102
```

Viewing the Configuration



Setup saves the configuration to NVRAM

show running and _show startup_ Commands
In RAM

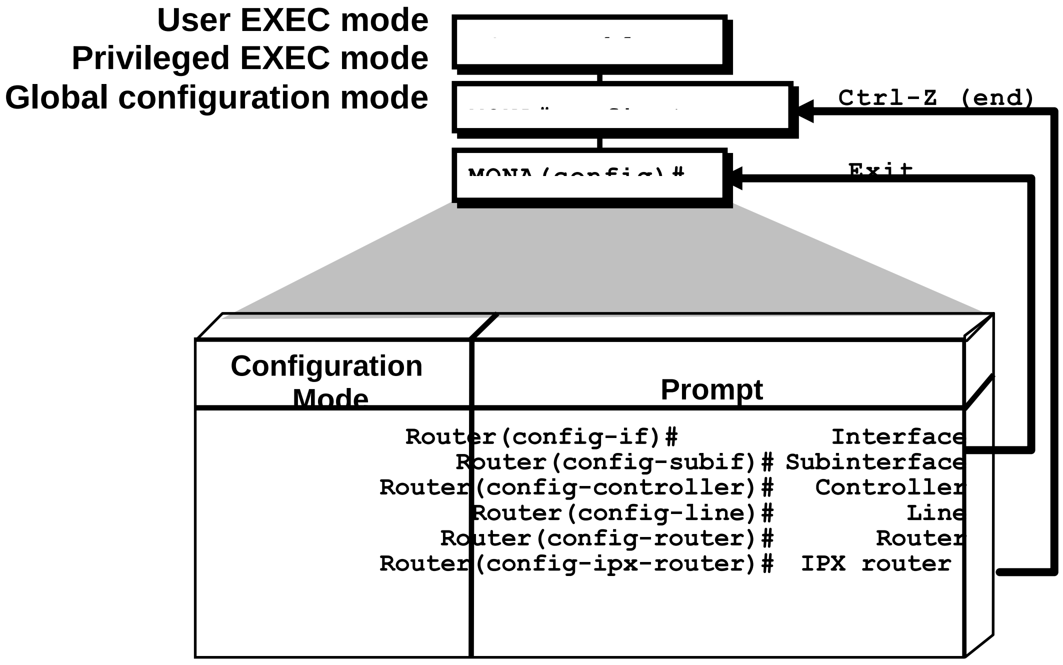
MONA#show running-config

```
Building configuration...
Current configuration:
!
version 12.0
!
        -- More --
```

In NVRAM
MONA#show startup-config

```
Using 1359 out of 32762 bytes
!
version 12.0
!
        -- More --
```

Overview of Router Modes



Configuration Mode	Prompt
Router(config-if)#	Interface
Router(config-subif)#	Subinterface
Router(config-controller)#	Controller
Router(config-line)#	Line
Router(config-router)#	Router
Router(config-ipx-router)#	IPX router

Saving Configurations
MONA#
MONA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
MONA#
Copy the current configuration to NVRAM

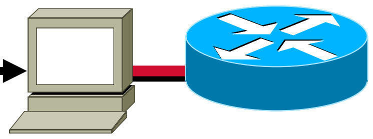
Configuring Router Identification

Router Name

```
Router(config)#hostname MONA
                 MONA(config)#
```

Message of the Day Banner

```
MONA(config)#banner motd #
Accounting Department
You have entered a secured
 system  Authorized access
```

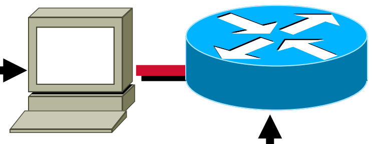


Configuring Router Identification

```
Router(config)#hostname MONA
                 MONA(config)#
```

Message of the Day Banner

```
wg_ro_c(config)#banner motd  #
   Accounting Department
   You have entered a secured
```



Interface Description

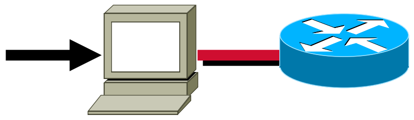
```
MONA(config)#interface ethernet 0
```

*Sets local identity or message for the accessed router or interface

Router Password Configuration

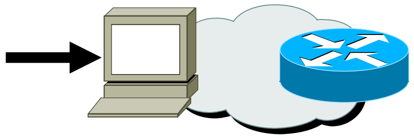
Console Password

```
MONA(config)#line console 0
   MONA(config-line)#login
```



Virtual Terminal Password

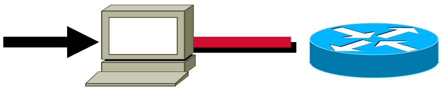
```
 MONA(config)#line vty 0 4
MONA(config-line)#login
```



Router Password Configuration

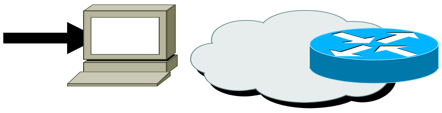
Console Password

```
MONA(config)#line console 0
     MONA(config-line)#login
```



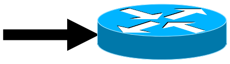
Virtual Terminal Password

```
Router(config)#line vty 0 4
 Router(config-line)#login
```



Enable Password

```
MONA(config)#enable password 1102011
```



Secret Password

```
MONA(config)#enable secret sanfran
```

Other Console Line Commands

MONA(config)#line console 0

MONA(config-line)#exec-timeout 0 0

*Prevents console session timeout

MONA(config)#line console 0

MONA(config-line)#logging synchronous

*Redisplays interrupted console input

Configuring an Interface

MONA(config)**#interface *type number***

MONA(config-if)#

*****type includes serial, ethernet, token ring, fddi, hssi, loopback, dialer, null, async, atm, bri, and tunnel

*number is used to identify individual interfaces

MONA(config)#interface *type slot/port*

MONA(config-if)#

*For modular routers

MONA(config-if)#exit

*Quit from current interface configuration mode

Configuring a Serial Interface

Enter global configuration mode

MONA#configure term

MONA(config)#

Specify interface

MONA(config)#interface serial 0

MONA(config-if)#

Configuring a Serial Interface

Enter global configuration mode

```
MONA#configure term
    Router(config)#
```

Specify interface

```
MONA(config)#interface serial 0
                MONA(config-if)#
```

Set clock rate (on DCE interfaces only)

```
MONA(config-if)#clock rate 64000
                MONA(config-if)#
```

Set bandwidth (recommended)

```
MONA(config-if)#bandwidth 64
        MONA(config-if)#exit
           MONA(config)#exit
                       MONA#
```

Verifying Your Changes

MONA#show interface serial 0

```
Serial0 is up, line protocol is up
 Hardware is HD64570
 Internet address is 10.140.4.2/24
 MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
 Last input 00:00:09, output 00:00:04, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0 (size/max/drops); Total output drops: 0
 Queueing strategy: weighted fair
 Output queue: 0/1000/64/0 (size/max total/threshold/drops)
   Conversations  0/1/256 (active/max active/max total)
   Reserved Conversations 0/0 (allocated/max allocated)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
```

(*output omitted)*

Ethernet media-type Command

MONA(config)#interface ethernet 2

MONA(config-if)#media-type 10baset

Select the media-type connector for the Ethernet interface

Disabling or Enabling an Interface

MONA#configure term

MONA(config)#interface serial 0

MONA(config-if)#shutdown

%LINK-5-CHANGED: Interface Serial0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down

Administratively turns off an interface

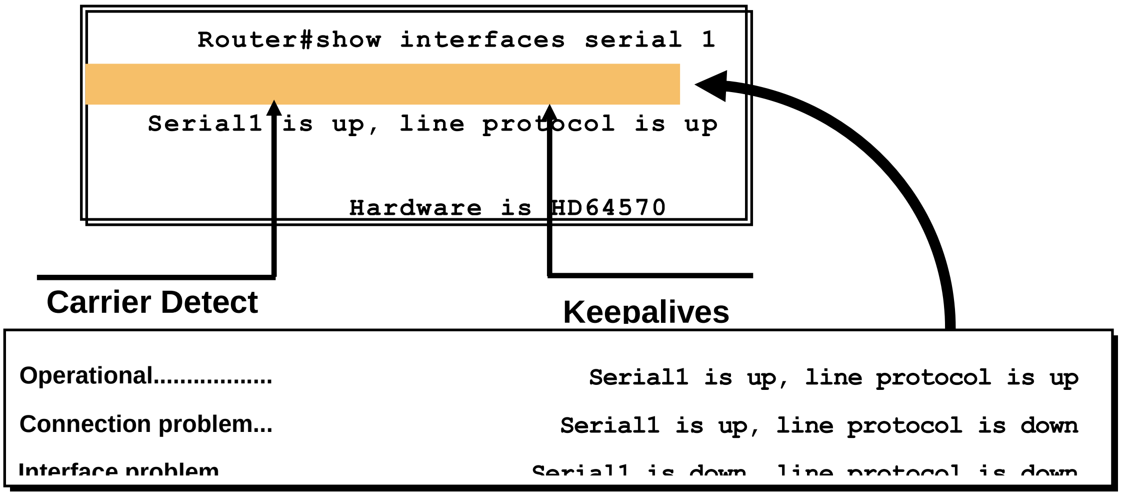
```
MONA#configure term
MONA(config)#interface serial 0
MONA(config-if)#no shutdown
%LINK-3-UPDOWN:  Interface Seria0, changed state to up
%LINEPROTO-5-UPDOWN:  Line Protocol on Interface Serial0, changed state to up
```

Enables an interface that is administratively shutdown

Router show interfaces Command

```
MONA#show interfaces
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e5d.ae2f (bia 00e0.1e5d.ae2f)
  Internet address is 10.1.1.11/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     81833 packets input, 27556491 bytes, 0 no buffer
     Received 42308 broadcasts, 0 runts, 0 giants, 0 throttles
     1 input errors, 0 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort
     0 input packets with dribble condition detected
     55794 packets output, 3929696 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 4 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Interpreting Interface Status



```
Router#show interfaces serial 1
Serial1 is up, line protocol is up
Hardware is HD64570
```

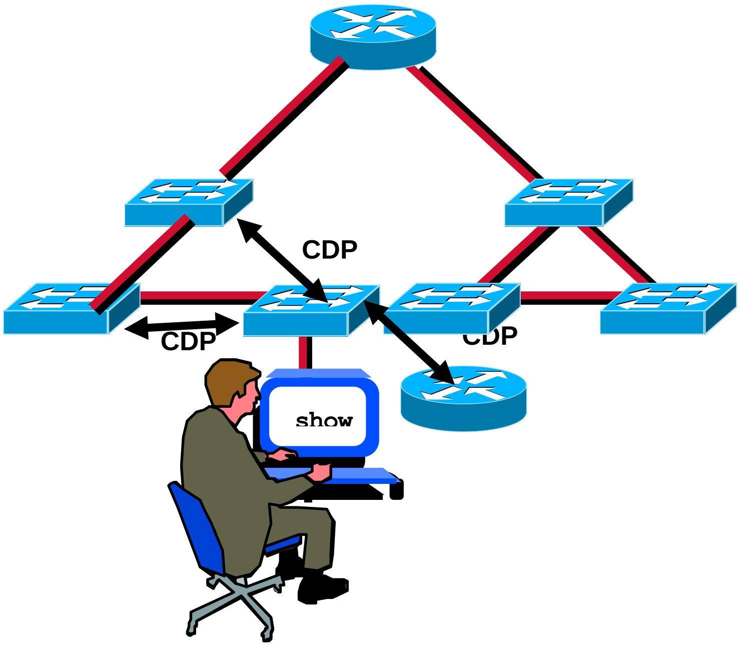
```
Operational..................     Serial1 is up, line protocol is up
Connection problem...             Serial1 is up, line protocol is down
Interface problem                 Serial1 is down, line protocol is down
```

Serial Interface show controller Command

```
MONA#show controller serial 0
        HD unit 0, idb = 0x121C04, driver structure at 0x127078
        buffer size 1524  HD unit 0, V.35 DTE cable
```

. Shows cable type of serial cables

Discovering Neighbors with CDP

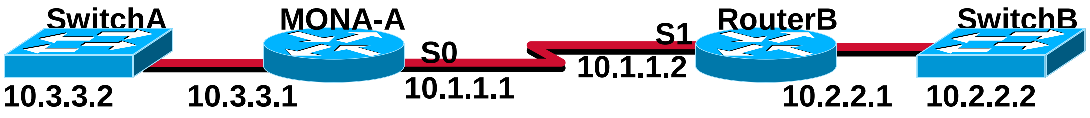


Runs on routers with Cisco IOS 10.3 or later and Cisco switches and hubs

Summary information includes:

*Device identifiers
*Address list
*Port identifier
*Capabilities list
*Platform

Using CDP

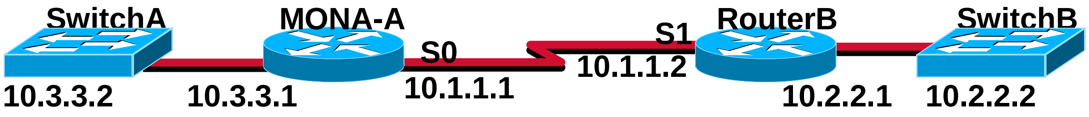


MONA-A#sh cdp ?

```
entry      Information for specific neighbor entry
interface  CDP interface status and configuration
neighbors  CDP neighbor entries
traffic    CDP statistics
<cr>
```

```
MONA-A(config)#no cdp run
MONA-A(config)#interface serial0
MONA-A(config-if)#no cdp enable
```

Using the show cdp neighbor Command

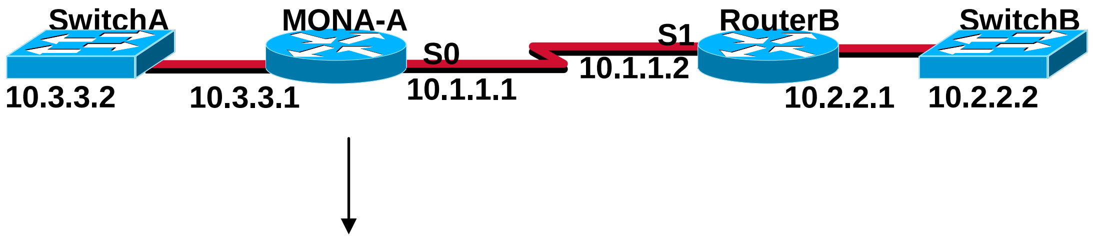


MONA-A#sh cdp neighbors

```
        Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                          S - Switch, H - Host, I - IGMP, r - Repeater
        Device ID       Local Intrfce     Holdtme    Capability  Platform  Port ID
RouterB           Ser 0          148          R         2522       Ser 1
        SwitchA0050BD855780 Eth 0         167          T S       1900      2
```

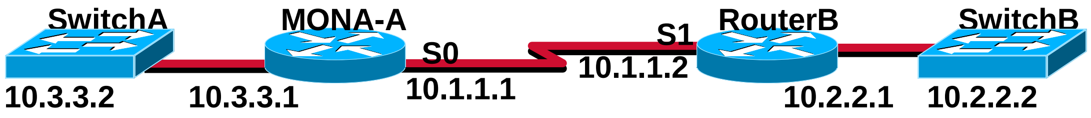
SwitchA also provides its Mac address

Using the show cdp entry Command



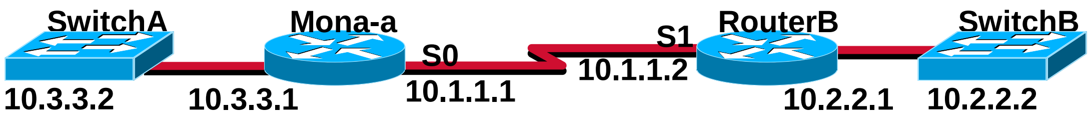
```
MONA-A#sh cdp entry *
-------------------------
Device ID: RouterB
        Entry address(es):
          IP address: 10.1.1.2
        Platform: cisco 2522,  Capabilities: Router
        Interface: Serial0,  Port ID (outgoing port): Serial1
        Holdtime : 168 sec

Version :
        Cisco Internetwork Operating System Software
        IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fci)
        Copyright (c) 1986-1999 by cisco Systems, Inc.
        Compiled Mon 08-Feb-99 18:18 by phanguye
```

Additional CDP Commands



```
MONA-A#sh cdp traffic
CDP counters :
              Packets output: 56, Input: 38
              Hdr syntax: 0, Chksum error: 0, Encaps failed: 3
              No memory: 0, Invalid packet: 0, Fragmented: 0
MONA-A#sh cdp interface
        BRI0 is administratively down, line protocol is down
          Encapsulation HDLC
          Sending CDP packets every 60 seconds
          Holdtime is 180 seconds
```

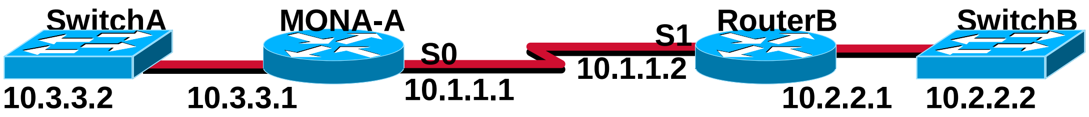
Using Telnet to Connect to Remote Devices



```
Mona-a#telnet 10.2.2.2
Trying 10.2.2.2 ... Open
------------------------------------------------
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address:      00-90-86-73-33-40
PCA Number:            73-2239-06
PCA Serial Number:     FAA02359H8K
Model Number:          WS-C1924-EN
System Serial Number:  FAA0237X0FQ
..
SwitchB>
```

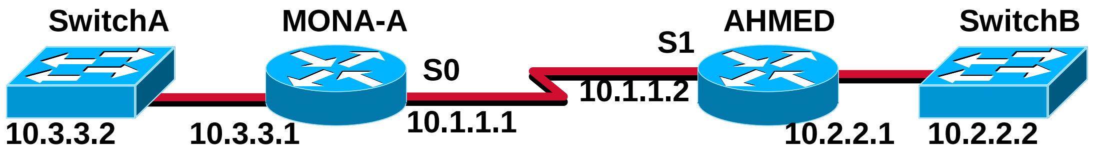
Remote device

Viewing Telnet Connections



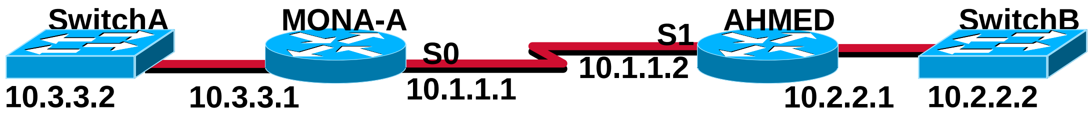
```
MONA-A#sh session
Conn Host              Address            Byte  Idle Conn Name
   1 10.1.1.2          10.1.1.2           0     1 10.1.1.2
*  2 10.3.3.2          10.3.3.2           0     0 10.3.3.2

MONA-A#sh user
    Line     User      Host(s)              Idle Location
*  0 con 0             10.1.1.2              3
                  10.3.3.2             2
  11 vty 0             idle                1 10.1.1.2
```

Suspending a Telnet Session



```
AHMED#<Ctrl-Shift-6>x
MONA-A#sh session
Conn Host            Address          Byte  Idle Conn Name
   1 10.1.1.2          10.1.1.2          0      1 10.1.1.2
MONA-A#resume 1
AHMED#
```

Closing a Telnet Session



```
MONA-A#disconnect
Closing connection to 10.3.3.2 [confirm]
```

Closing the current session opened by you

Closing a session opened by a remote device

```
MONA-A#clear line 11
[confirm]
 [OK]
```

Using the ping and trace Commands

```
MONA##ping 10.1.1.10
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
MONA#trace 10.1.1.10
        Type escape sequence to abort.
        Tracing the route to 10.1.1.10
          1 10.1.1.10 4 msec 4 msec 4 msec
MONA#
```

Test connectivity and path to a remote device

Router Power on/Bootup Sequence

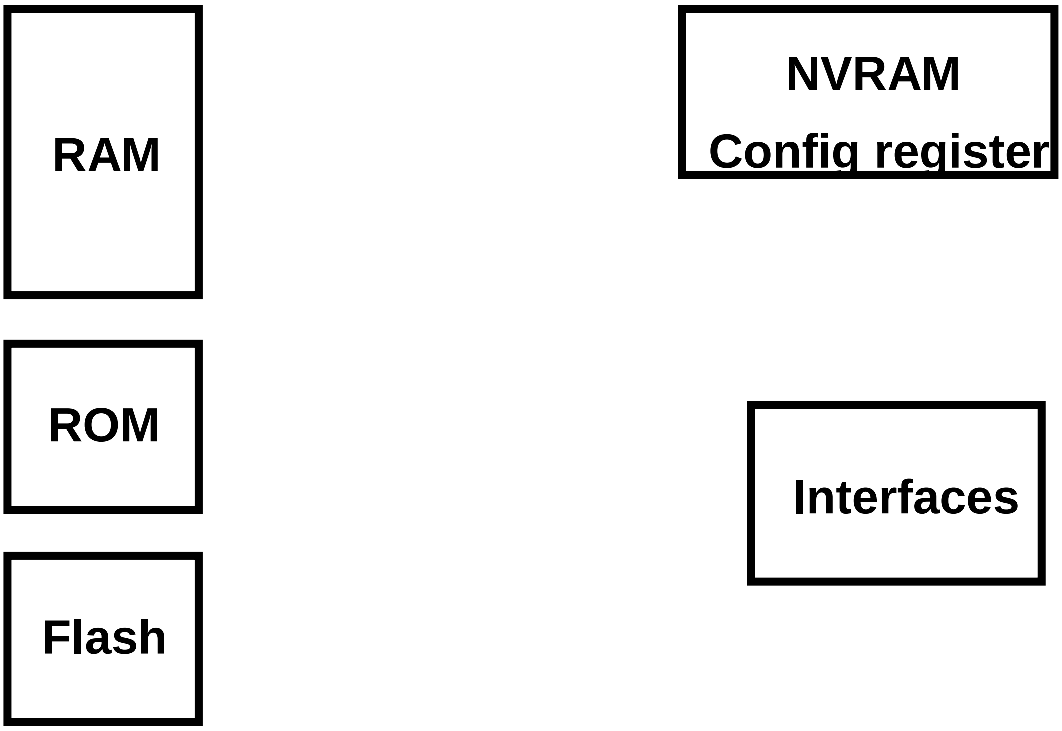
*Power on self test (POST)

*Load and run bootstrap code

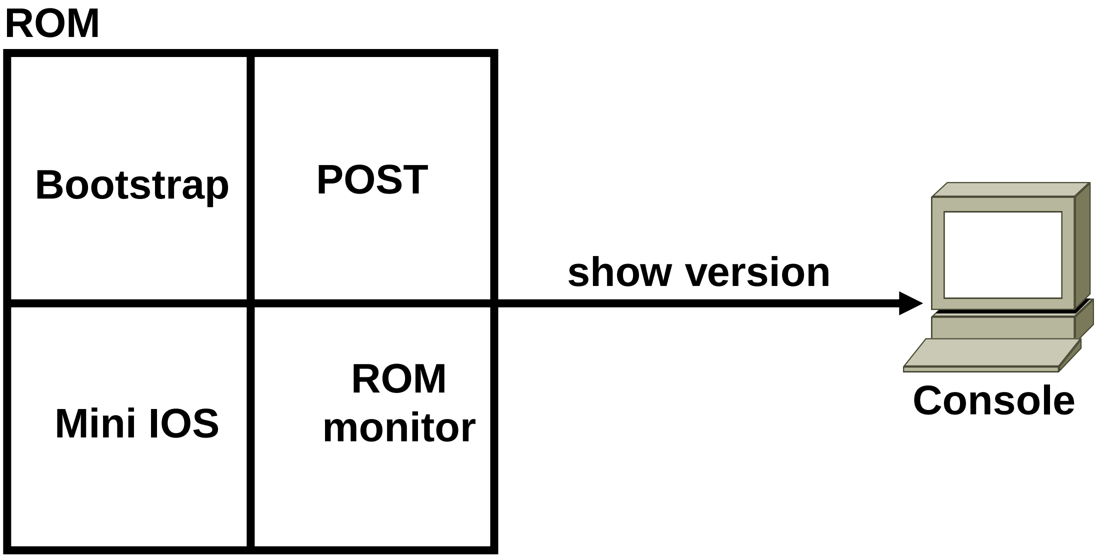
*Find the IOS software

*Load the IOS software
*Find the configuration
*Load the configuration
*Run

Router Internal Components

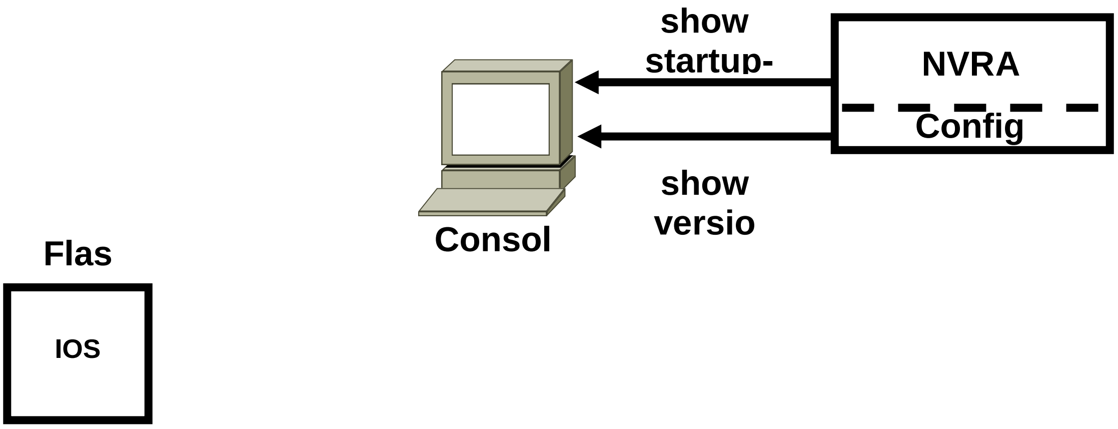


ROM Functions



Contains microcode for basic functions

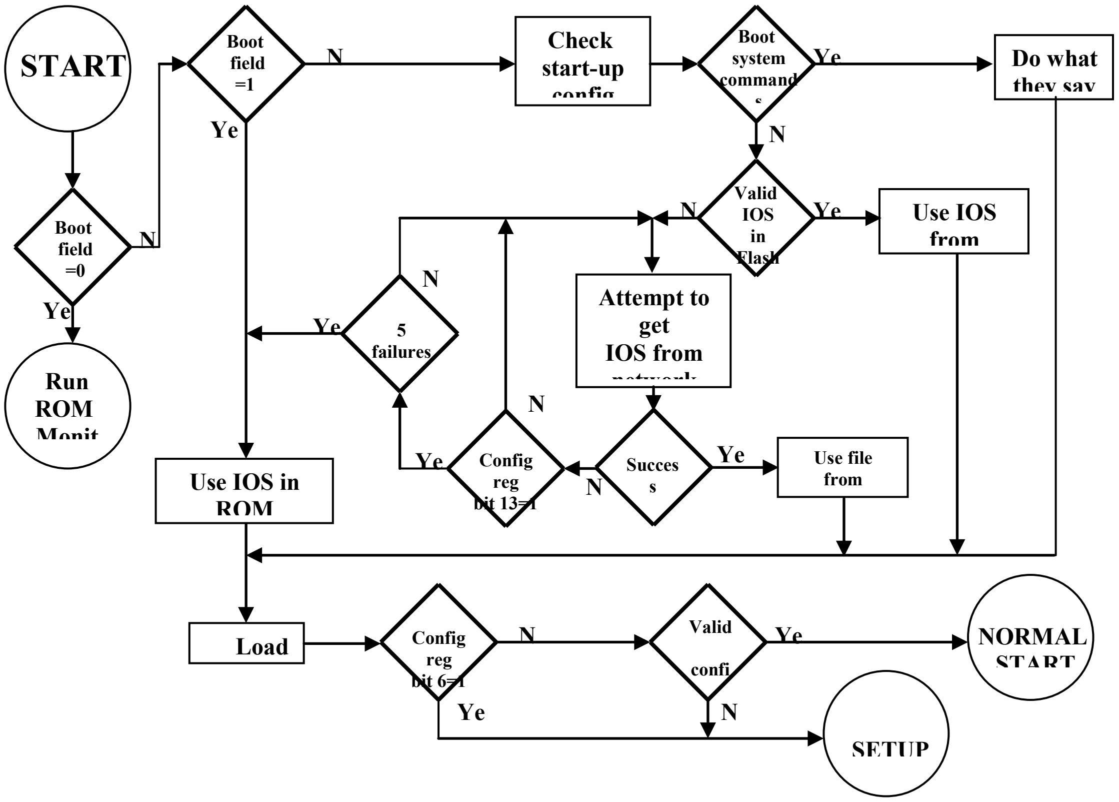
Finding the IOS



Order of search:

1. Check configuration register
2. Parse config in NVRAM
3. Default to first file in Flash
4. Attempt net boot
5. RXBOOT
6. ROMMON

Router Start-up Flow Chart



Determining the Current Configuration Register Value

```
MONA_a#show version
        Cisco Internetwork Operating System Software
        IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fc1)
        Copyright (c) 1986-1999 by cisco Systems, Inc.
        Compiled Mon 08-Feb-99 18:18 by phanguye
        Image text-base: 0x03050C84, data-base: 0x00001000
        ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
        BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE (fc1)
MONA uptime is 20 minutes
        System restarted by reload
        System image file is "flash:c2500-js-l_120-3.bin"
        --More--
Configuration register is 0x2102
```

Configuration register value in *show version*

Configuration Register Values

```
MONA#configure terminal
MONA(config)#config-register 0x2102
[Ctrl-Z]
MONA#reload
```

*Configuration register bits 3, 2, 1, and 0 set boot option

Configuration Register Values

```
MONA#configure terminal
MONA(config)#config-register 0x2102
[Ctrl-Z]
MONA#reload
```

Configuration Register Boot Field Value	Meaning
	Use ROM monitor mode (Manually boot using the b command)

Configuration Register Values

```
MONA#configure terminal
MONA(config)#config-register 0x2102
[Ctrl-Z]
MONA#reload
```

*Configuration register bits 3, 2, 1, and 0 set boot option

Configuration Register Boot Field Valu	Meaning
0x0	Use ROM monitor mode (Manually boot using the b Command)
0x1	Automatically boot from ROM(Provides IOS subset)

Configuration Register Values

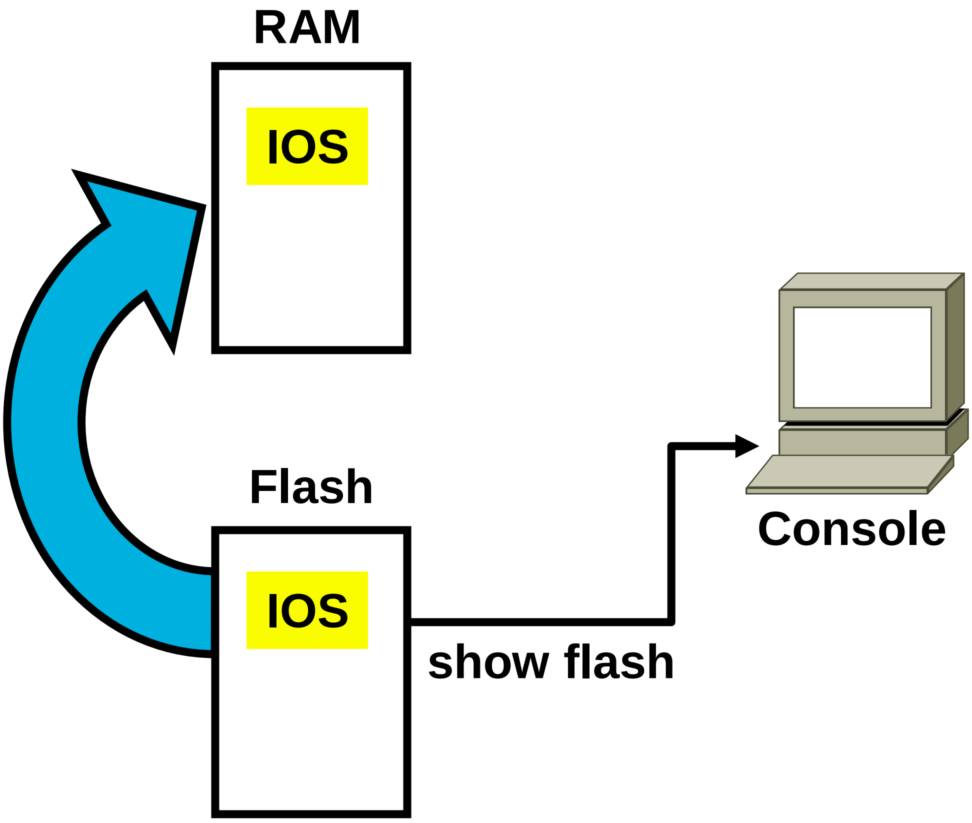
```
MONA#configure terminal
MONA(config)#config-register 0x2102
[Ctrl-Z]
MONA#reload
```

*Configuration register bits 3, 2, 1, and 0 set boot option

Configuration Register Boot Field Value	Meaning
0x0	Use ROM monitor mode (Manually boot using the b command)
0x1	Automatically boot from ROM (Provides IOS subset)
0x2 to 0xF	Examine NVRAM for boot system commands (0x2 default if router has Flash)

*Check configuration register value with show version

Loading the IOS from Flash

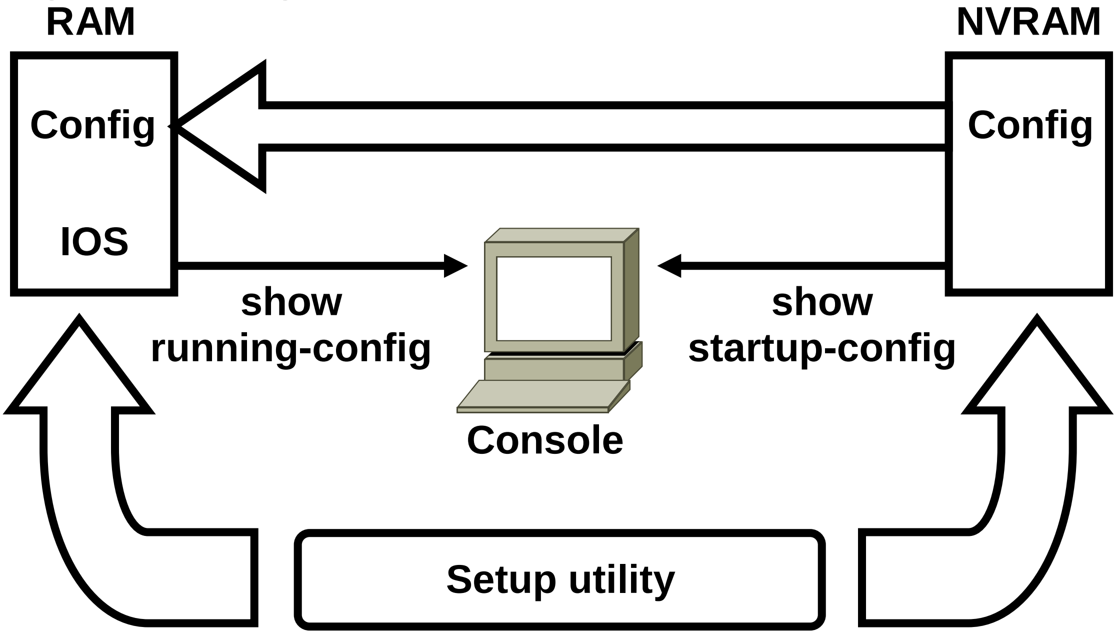


show flash **Command**

MONA#sh flash

```
System flash directory:
File  Length   Name/status
  1   10084696  c2500-js-l_120-3.bin
[10084760 bytes used, 6692456 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Loading the Configuration



show running and *show startup* Commands

In RAM

MONA#show running-config

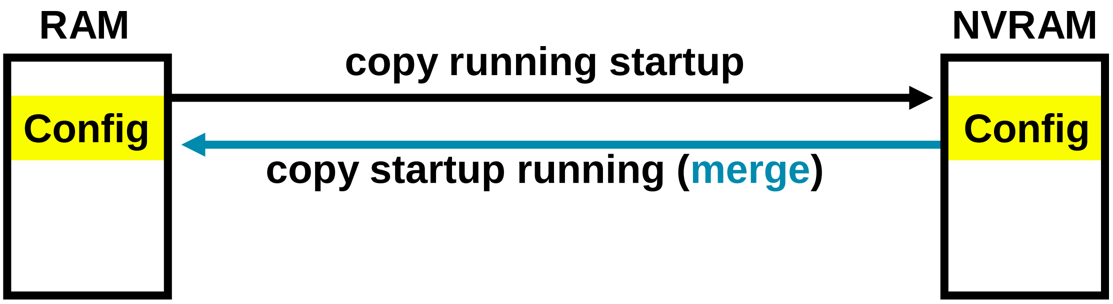
```
Building configuration...
Current configuration:
!
version 12.0
!
        -- More --
```

In NVRAM

MONA#show startup-config

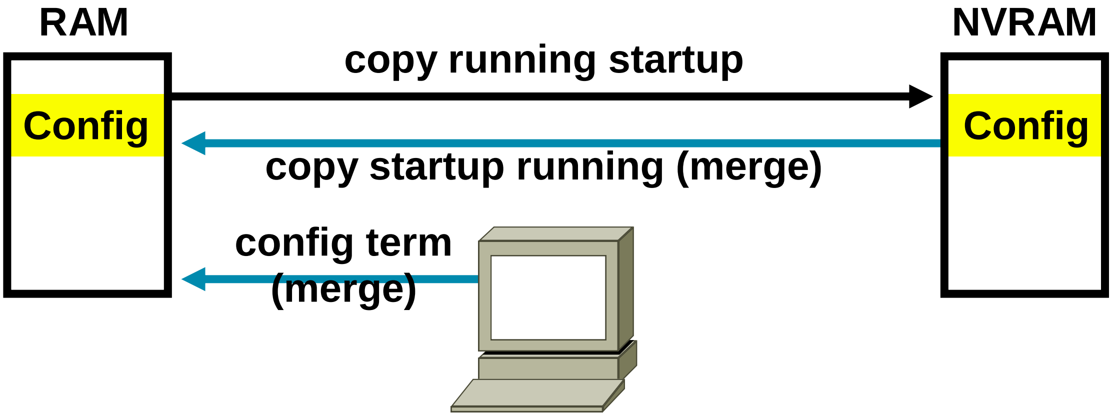
```
Using 1359 out of 32762 bytes
!
version 12.0
!
        -- More --
```

Sources of Configurations



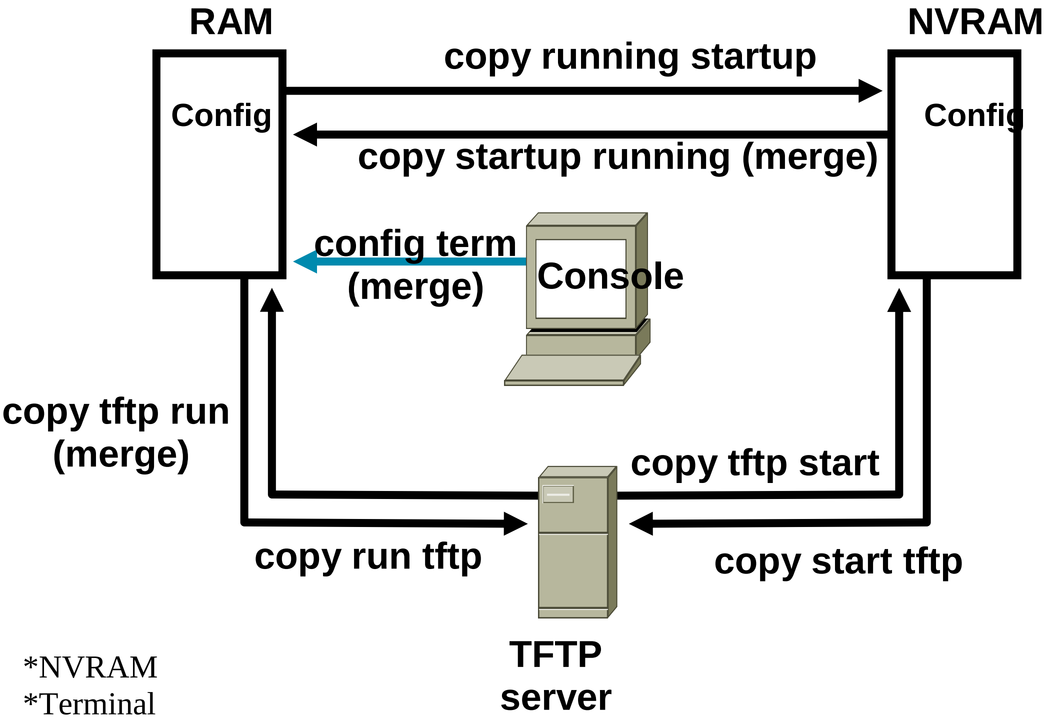
*NVRAM

Sources of Configurations



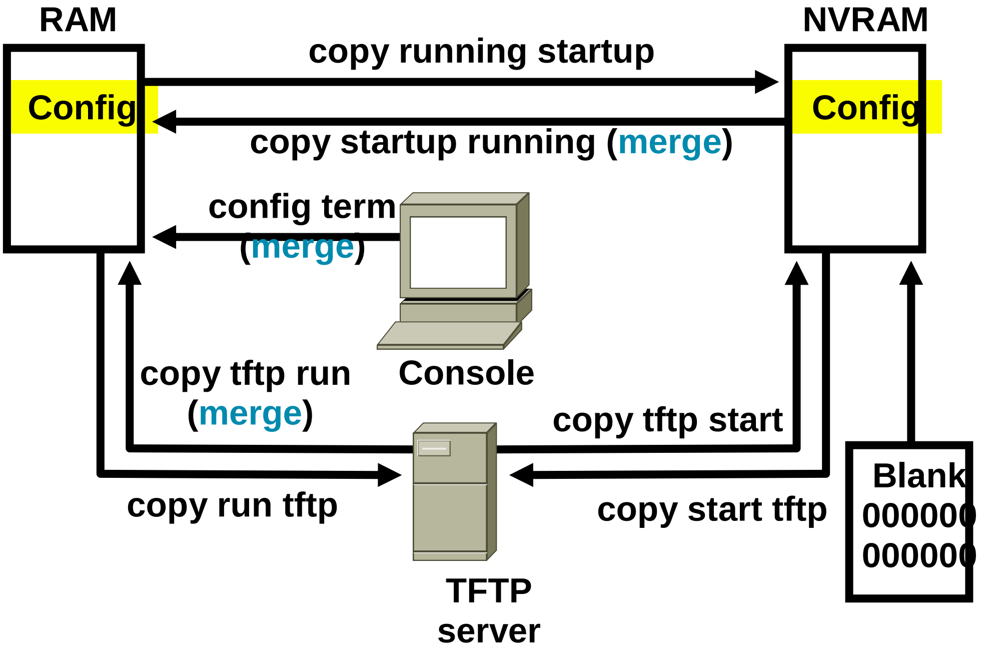
*NVRAM
*Terminal

Sources of Configurations



*NVRAM
*Terminal
*TFTP server

Sources of Configurations

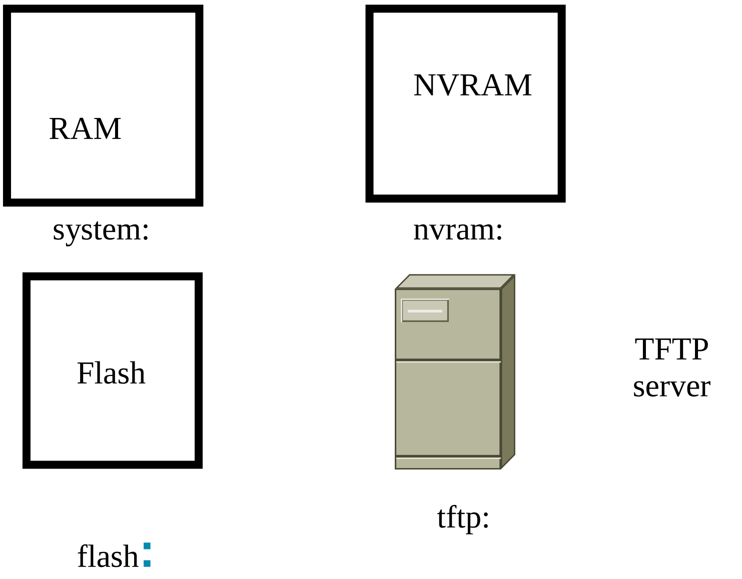


*NVRAM
*Terminal
*TFTP server
*Erase Start

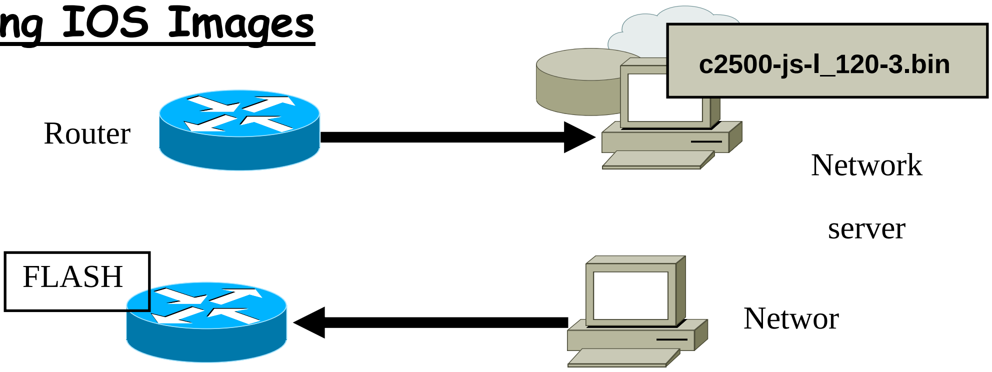
copy run tftp and copy tftp run Commands

```
MONA#copy running-config tftp
         Address or name of remote host []? 10.1.1.1
         Destination filename [running-config]? wgroa.cfg
         .!!
         1684 bytes copied in 13.300 secs (129 bytes/sec)
 MONA#copy tftp running-config
         Address or name of remote host []? 10.1.1.1
         Source filename []? wgroa.cfg
         Destination filename [running-config]?
         Accessing tftp://10.1.1.1/wgroa.cfg...
         Loading wgroa.cfg from 10.1.1.1 (via Ethernet0): !
         [OK - 1684/3072 bytes]
         1684 bytes copied in 17.692 secs (99 bytes/sec)
```

Cisco IOS File Systems and Devices



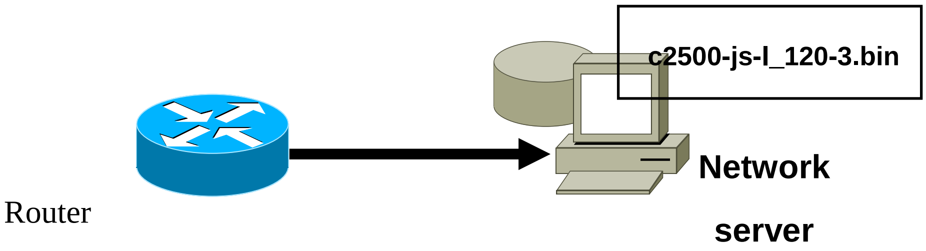
Managing IOS Images



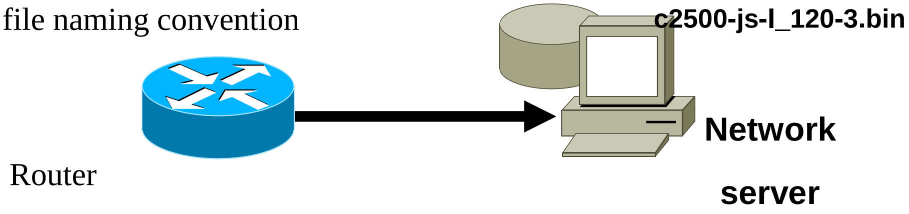
Preparing for a Network Backup Image

Router
Network
server

*Check access to the server
*Preparing for a Network Backup Image



*Check access to the server
*Check space available on the server
*Check file naming convention



*Check access to the server
*Check space available on the server
*Check file naming convention
*Create file on server if required

Verifying Memory and Deciphering Image Filenames

```
MONA#show flash
        System flash directory:
        File  Length   Name/status
          1   10084696  c2500-js-l_120-3.bin
        [10084760 bytes used, 6692456 available, 16777216 total]
        16384K bytes of processor board System flash (Read ONLY)
```

Verify Flash memory has room for the IOS image

Creating a Software Image Backup

```
MONA#copy flash tftp
        Source filename []? c2500-js-l_120-3.bin
        Address or name of remote host []? 10.1.1.1
        Destination filename [c2500-js-l_120-3.bin]?
        !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
        10084696 bytes copied in 709.228 secs (14223 bytes/sec)
MONA#
```

Upgrading the Image from the Net

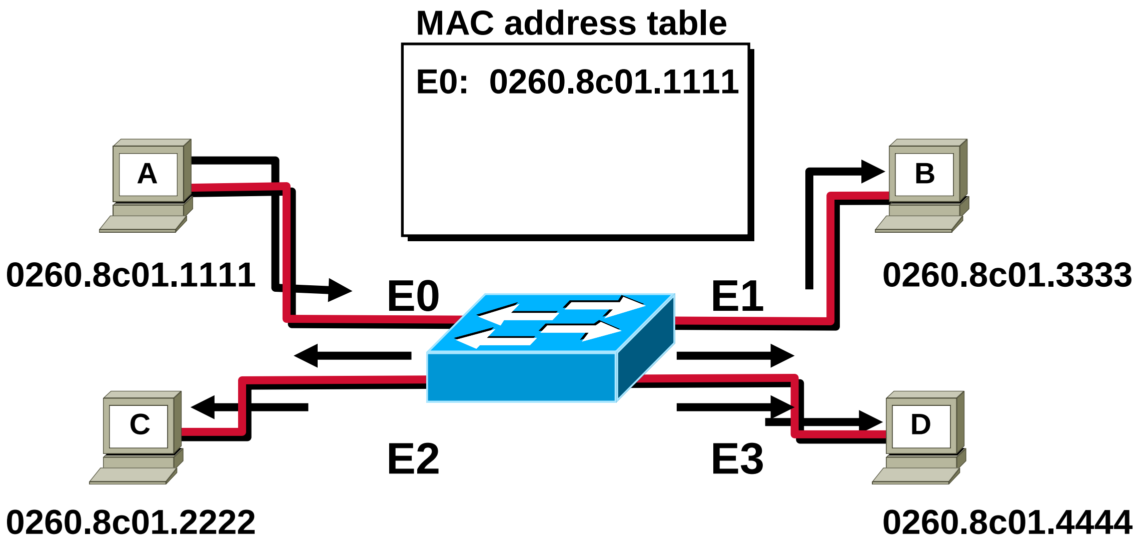
```
MONA#copy tftp flash
        Address or name of remote host [10.1.1.1]?
        Source filename []? c2500-js-l_120-3.bin
        Destination filename [c2500-js-l_120-3.bin]?
        Accessing tftp://10.1.1.1/c2500-js-l_120-3.bin...
        Erase flash: before copying? [confirm]
        Erasing the flash filesystem will remove all files! Continue? [confirm]
        Erasing device... eeeee (output omitted) ...erased
        Erase of flash: complete
        Loading c2500-js-l_120-3.bin from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!!!!!
(output omitted)
        [OK - 10084696/20168704 bytes]
        Verifying checksum...  OK (0x9AA0)
        10084696 bytes copied in 309.108 secs (32636 bytes/sec)
MONA#
```

*Erase Flash occurs before loading new image

*Note message that image already exists

Switch

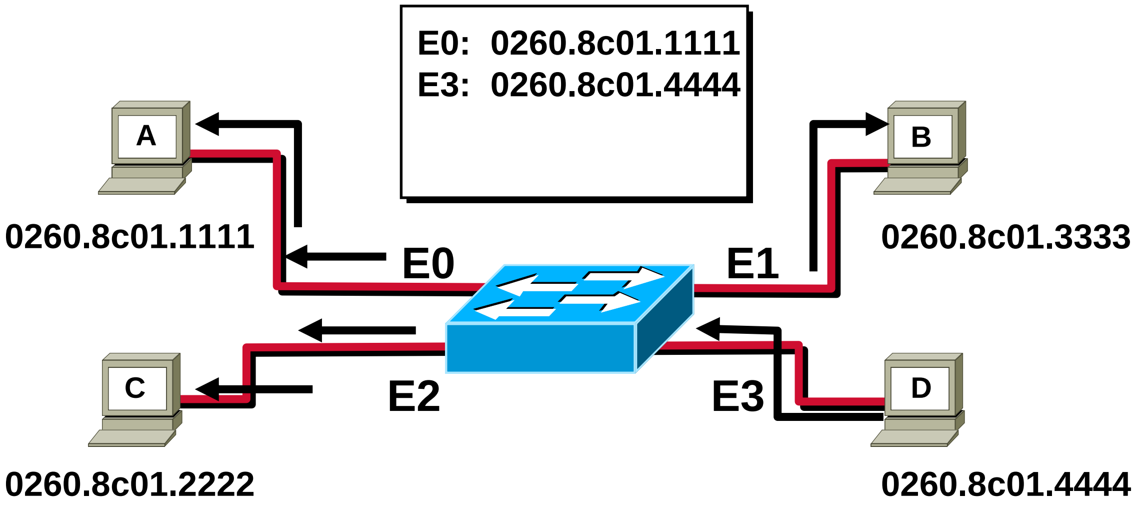
How Switches Learn Hosts Locations


MAC address table

E0: 0260.8c01.1111

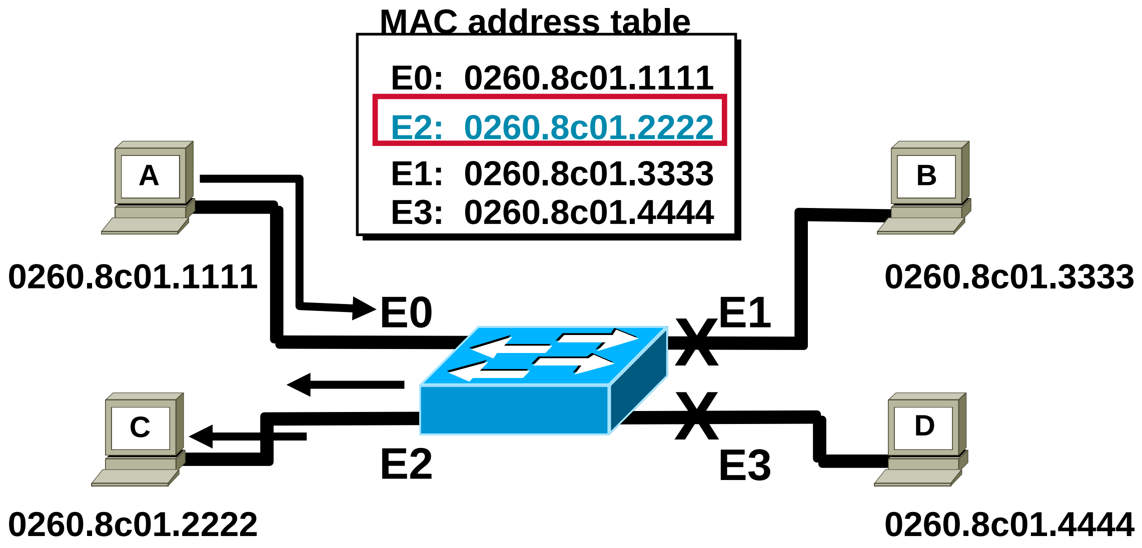
*Station A sends a frame to Station C
*Switch caches station A MAC address to port E0 by learning the source address of data frames
*The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded)

How Switches Learn Host Locations

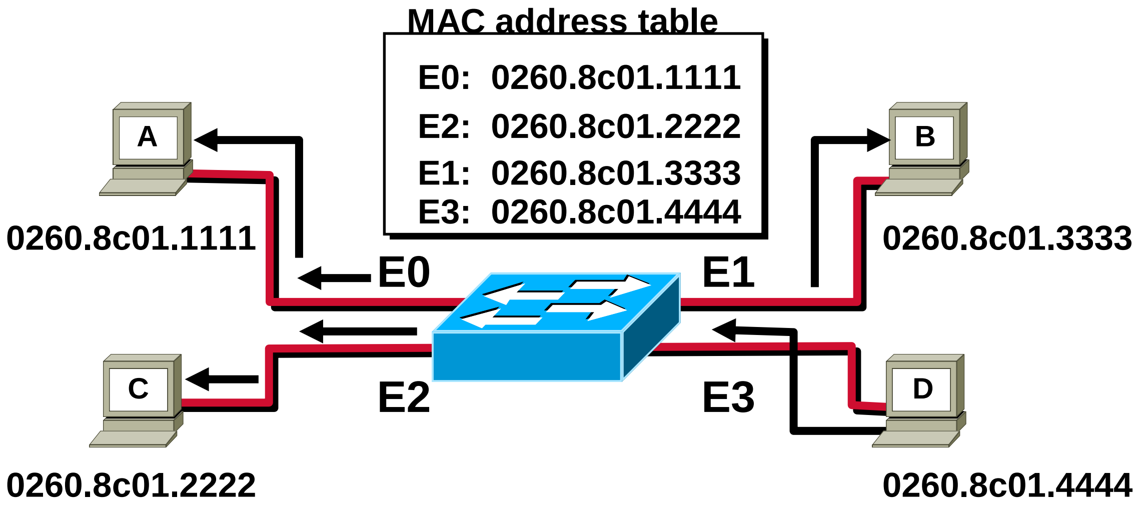

E0: 0260.8c01.1111
E3: 0260.8c01.4444

*Station D sends a frame to station C
*Switch caches station D MAC address to port E3 by learning the source Address of data frames
*The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded)

How Switches Filter Frames

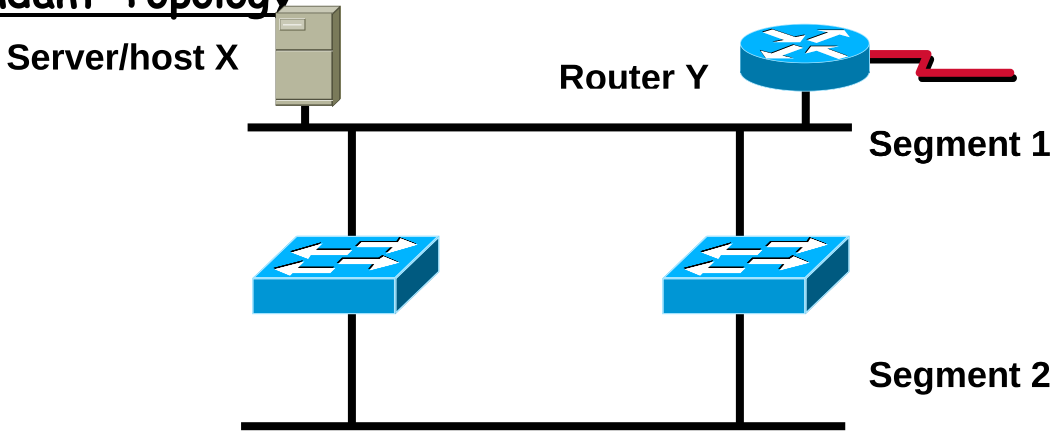


Broadcast and Multicast Frames



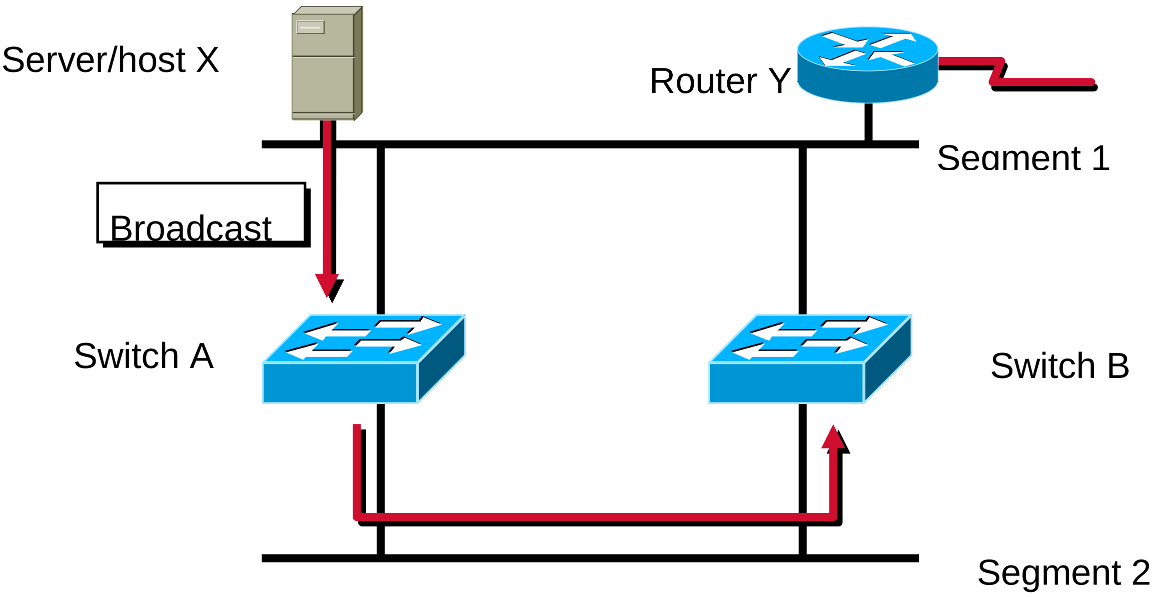
*Station D sends a broadcast or multicast frame
*Broadcast and multicast frames are flooded to all ports other than the originating port

Redundant Topology



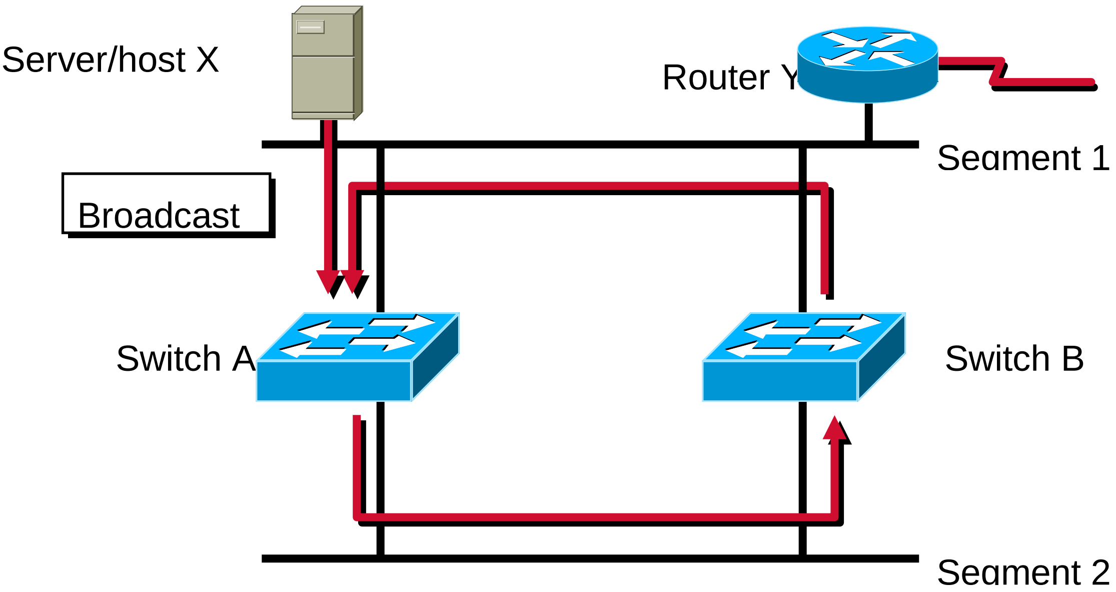
*Redundant topology eliminates single points of failure
*Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems

Broadcast Storms



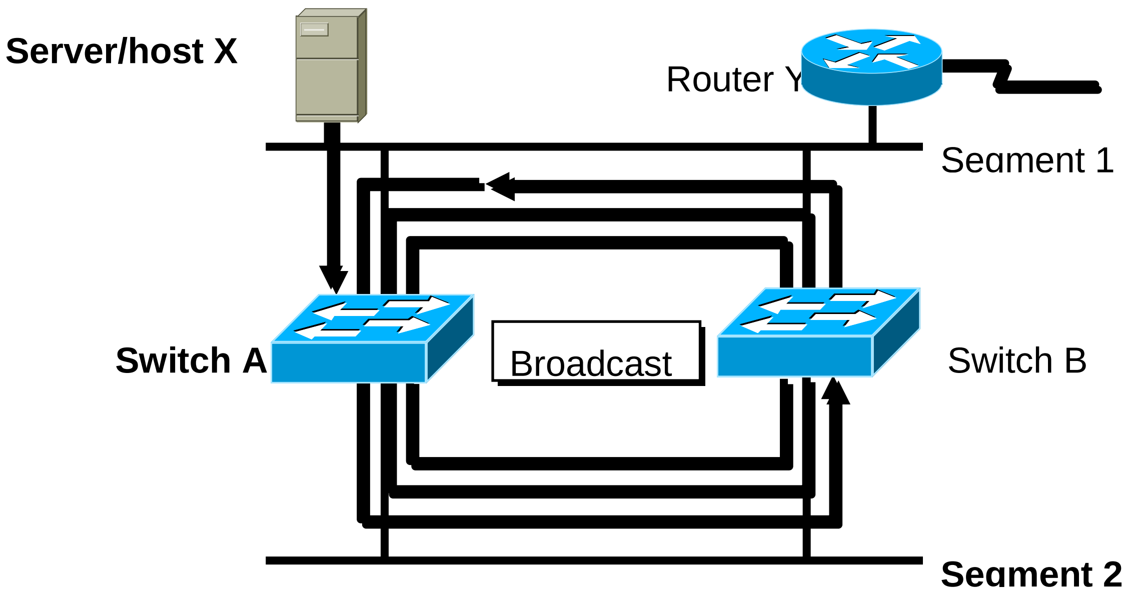
Host X sends a Broadcast

Broadcast Storms

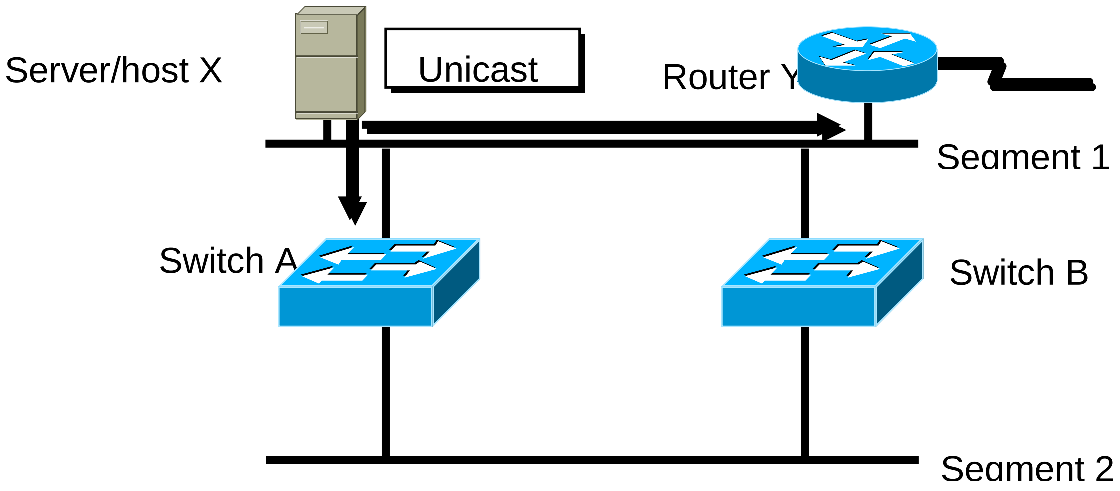


Host X sends a Broadcast

Broadcast Storms

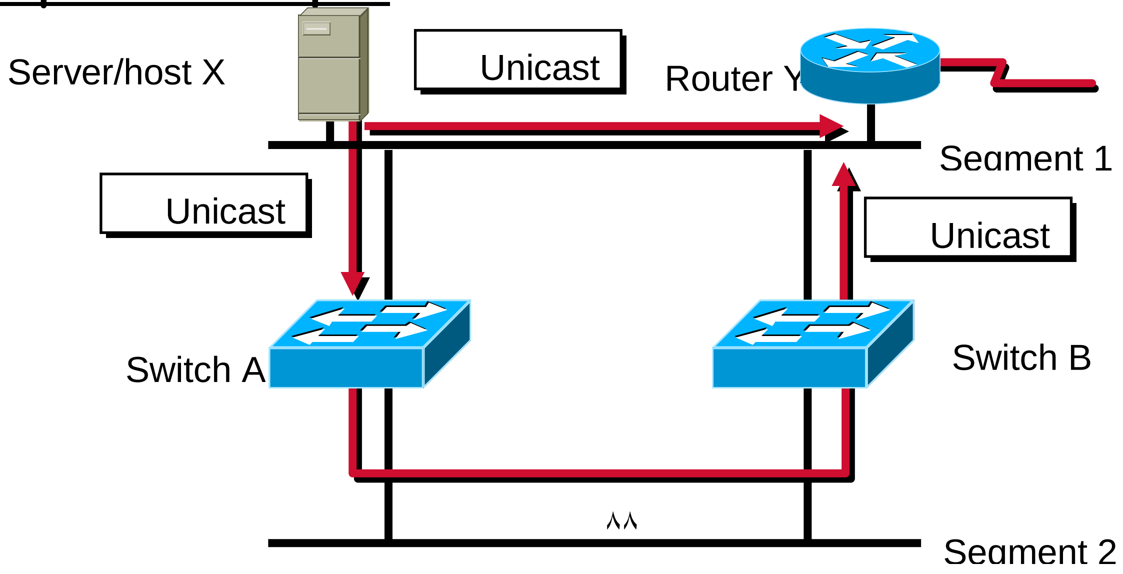


Multiple Frame Copies



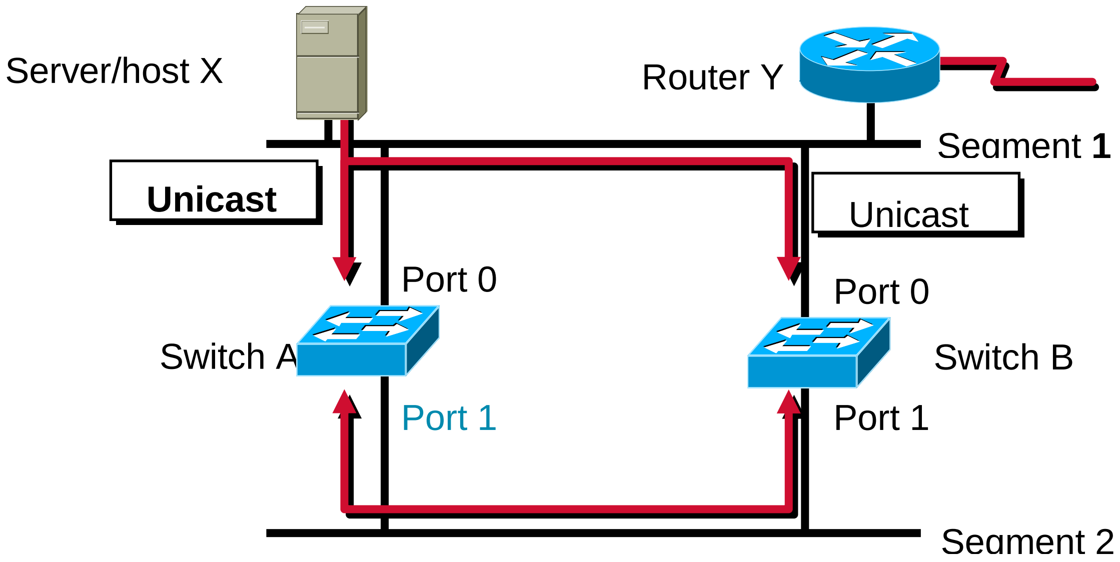
*Host X sends an unicast frame to router Y
*Router Y MAC address has not been learned by either switch yet

Multiple Frame Copies



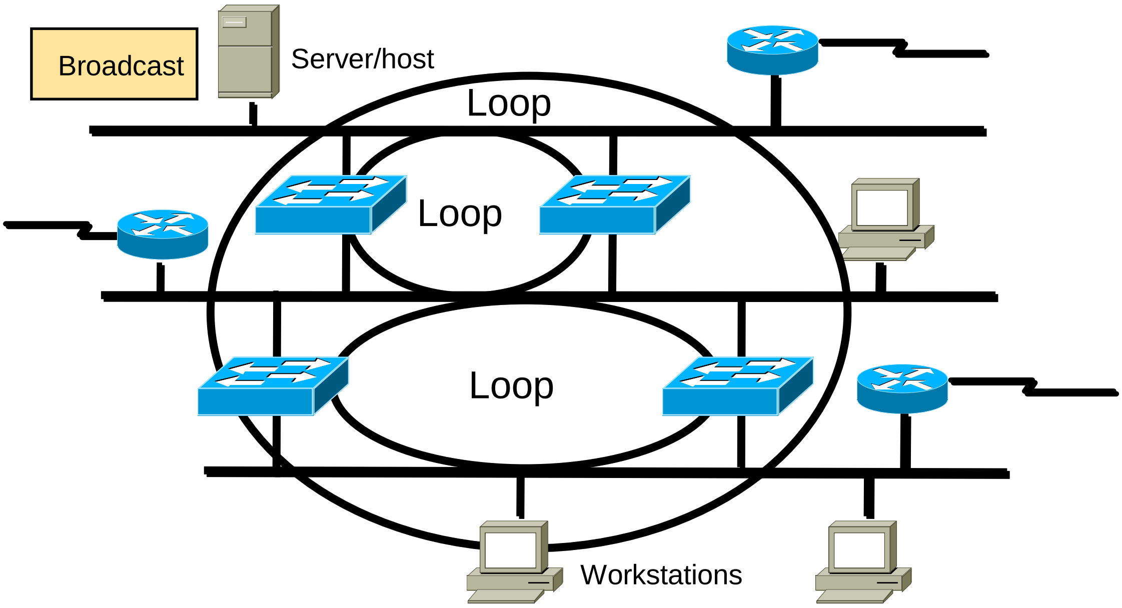
*Host X sends an unicast frame to Router Y
*Router Y MAC Address has not been learned by either Switch yet
*Router Y will receive two copies of the same frame

MAC Database Instability



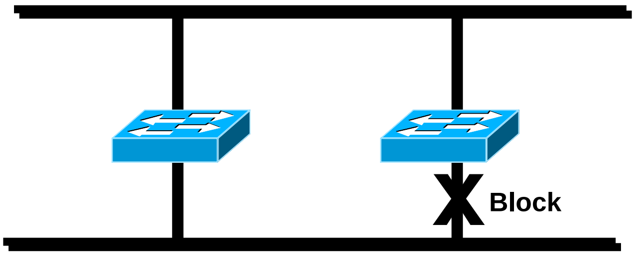
*Host X sends an unicast frame to Router Y
*Router Y MAC Address has not been learned by either Switch yet
*Switch A and B learn Host X MAC address on port 0
*Frame to Router Y is flooded
*Switch A and B incorrectly learn Host X MAC address on port 1

Multiple Loop Problems



*Complex topology can cause multiple loops to occur
* has no mechanism to stop the loop

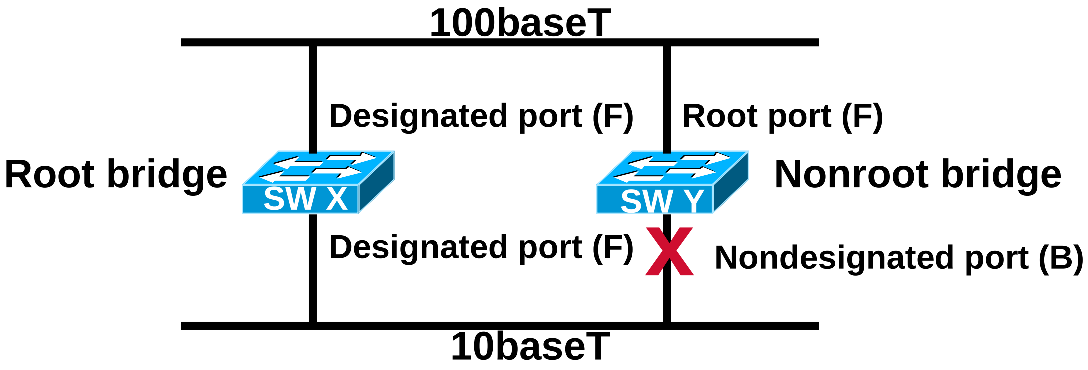
Spanning-Tree Protocol



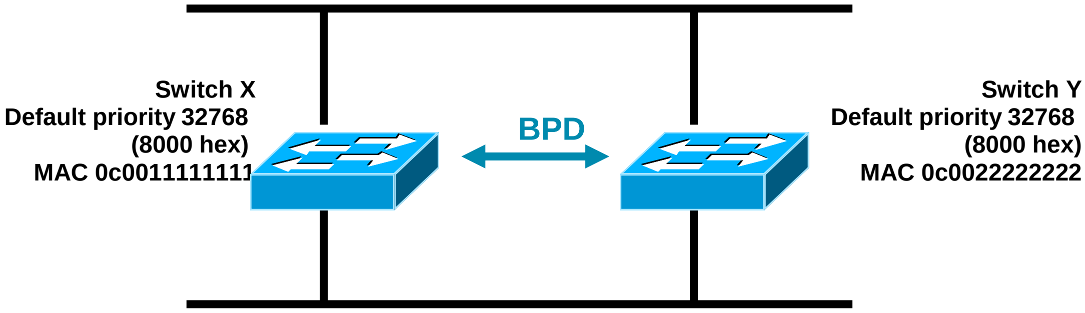
*Provides a loop free redundant network topology by
*placing certain ports in the blocking state

Spanning-Tree Operations

*One root bridge per network
*One root port per nonroot bridge
*One designated port per segment

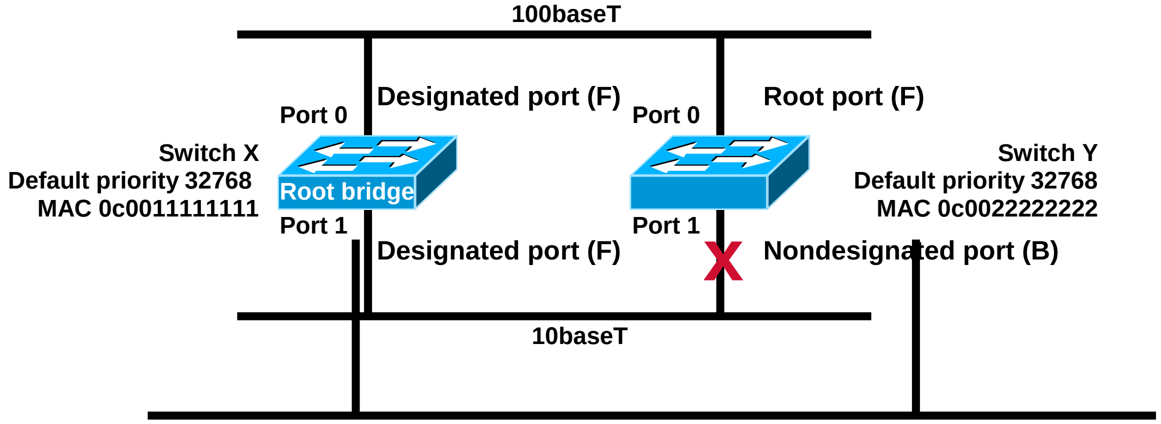


Tree Protocol Root Bridge Selection



BPDU = Bridge protocol data unit
(default = sent every 2 seconds)
Root bridge = Bridge with the lowest bridge ID
Bridge ID = Bridge priority + bridge MAC address
In the example, which switch has the lowest bridge ID?

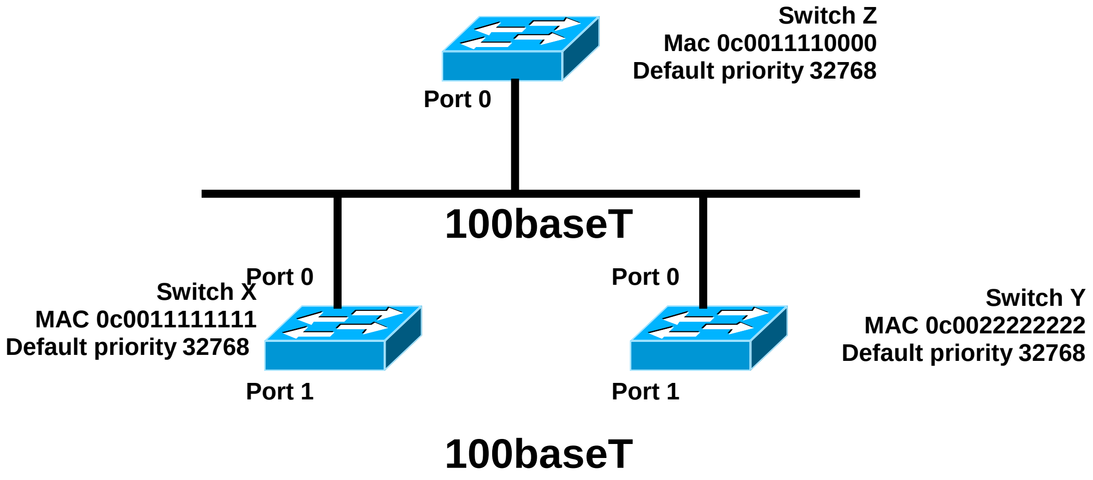
Spanning-Tree Protocol Port States



Spanning-Tree Protocol Path Cost

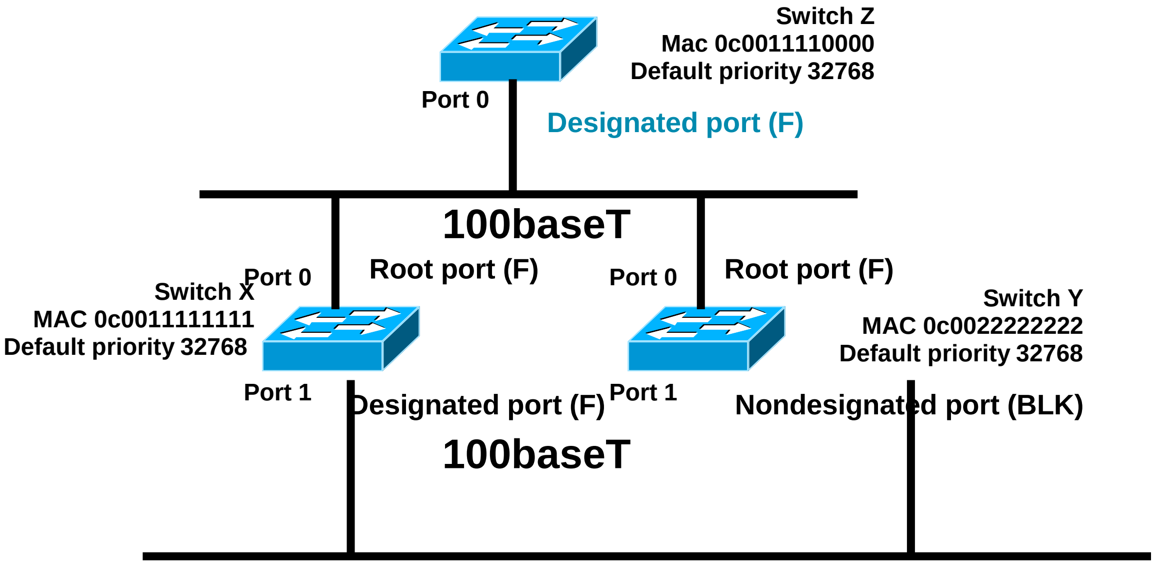
Link Speed	Cost (reratify IEEE spec)	Cost (previous IEEE spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Spanning-Tree:



Can you figure out:
*What is the root bridge?
*What are the designated, nondesignated, and root parts?
*Which are the forwarding and blocking ports?

Spanning-Tree:



Can you figure out:

*What is the root bridge?

*What are the designated, nondesignated, and root parts?

*Which are the forwarding and blocking ports?

Spanning-Tree Port States

Spanning-tree transitions each port through several different state:

Blocking

↓

Listening

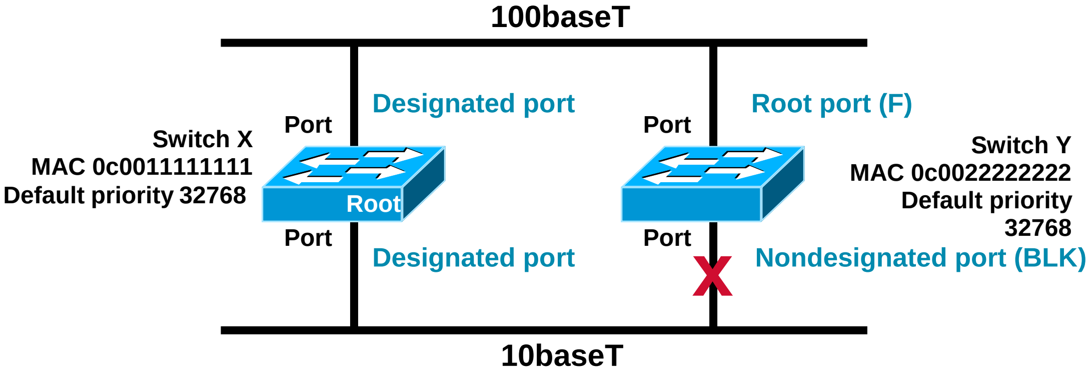
↓

Learning

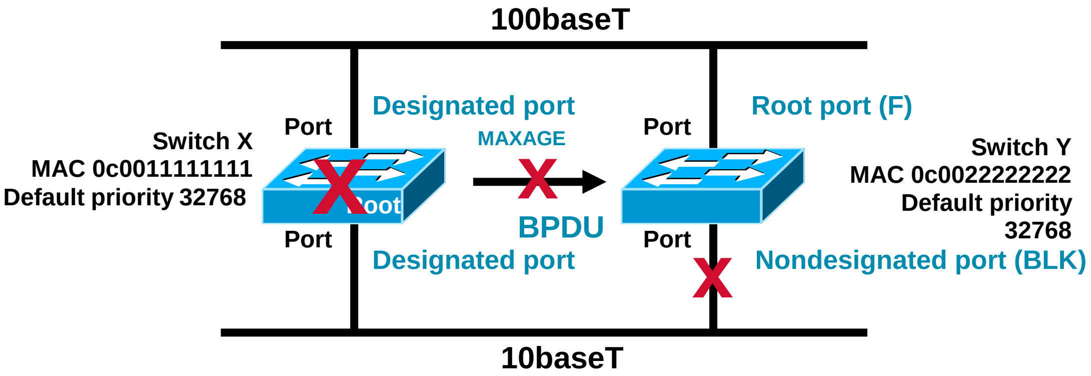
↓

Forwarding

Spanning-Tree Recalculation



Spanning-Tree Recalculation



Key Issue: Time to Convergence

*Convergence occurs when all the switches and bridge ports have transitioned to either the forwarding or blocking state

*When network topology changes, switches and bridges must recompute the Spanning-Tree Protocol, which disrupts user traffic

Bridging Compared to LAN Switching

Bridging

Primarily software based
One spanning-tree instance per bridge
Usually up to 16 ports per bridge

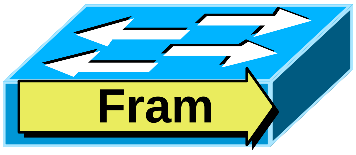
LAN Switching

Primarily hardware based (ASIC)
Many spanning-tree instances per switch
More ports on a switch

Transmitting Frames Through a Switch

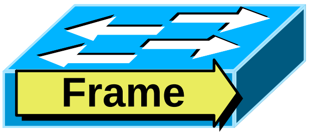
Cut-through

*Switch checks destination address and immediately begins forwarding frame

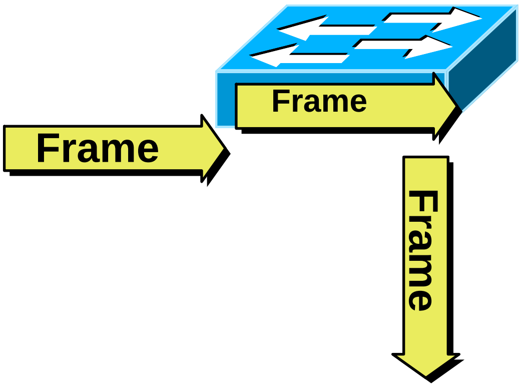


Transmitting Frames through a Switch

Cut-through
Switch checks destination address and
immediately begins forwarding frame



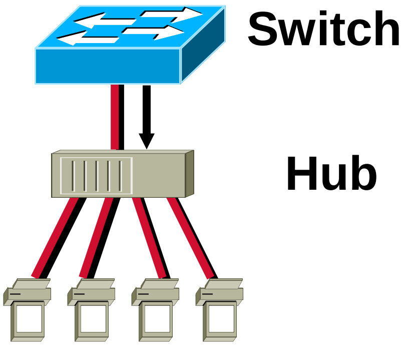
Store and forward
Complete frame is received and checked before
forwarding



Duplex Overview

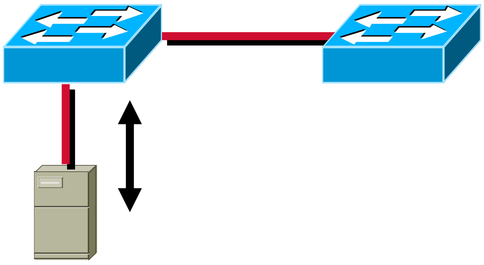
Half duplex (CSMA/CD)
*Unidirectional data flow
*Higher potential for collison
*Hubs connectivity

Duplex Overview



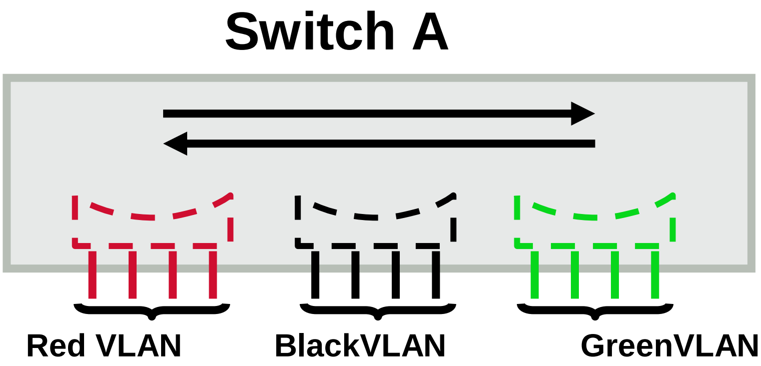
Half duplex (CSMA/CD)
*Unidirectional data flow
*Higher potential for collison
*Hubs connectivity

Full duplex
*Point-to-point only
*Attached to dedicated switched port
*Requires full-duplex support on both ends
*Collision free
*Collision detect circuit disabled



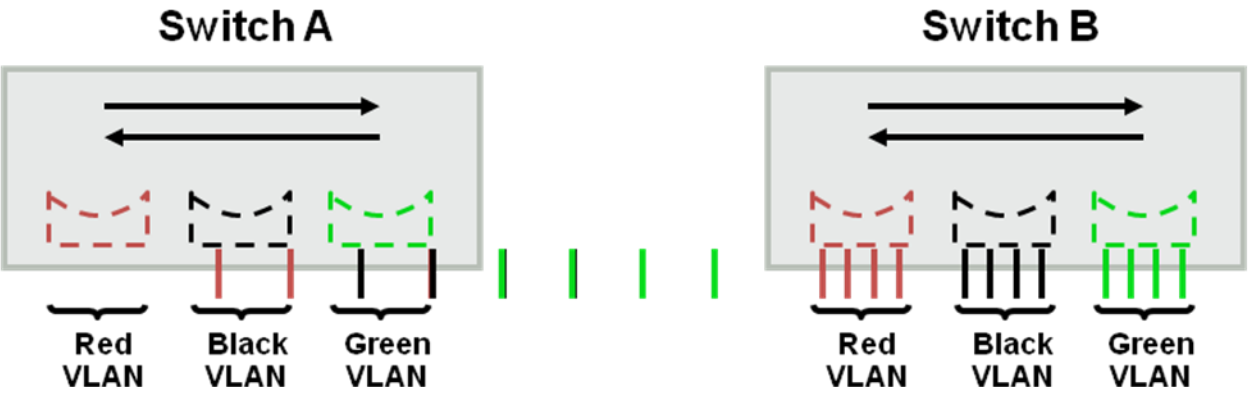
VLAN

VLAN Operations



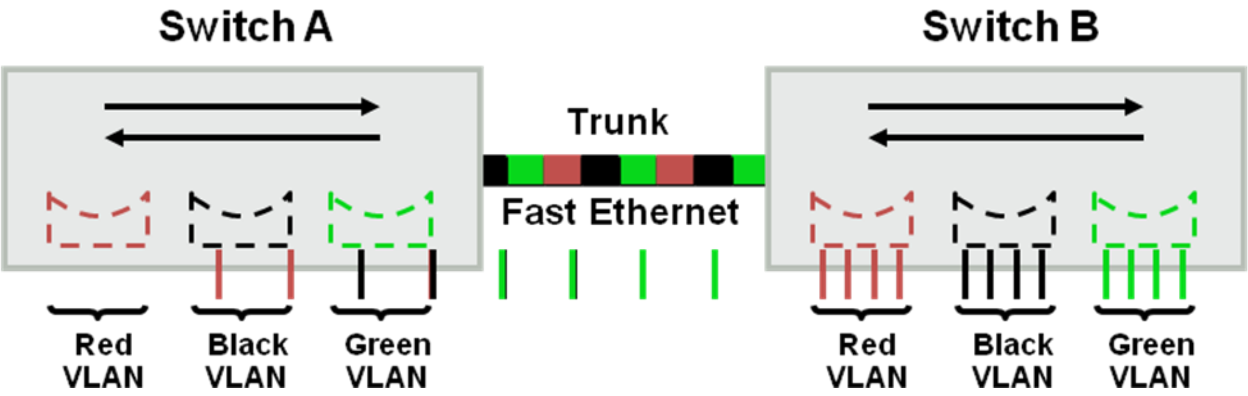
*Each logical VLAN is like a separate physical bridge

VLAN Operations



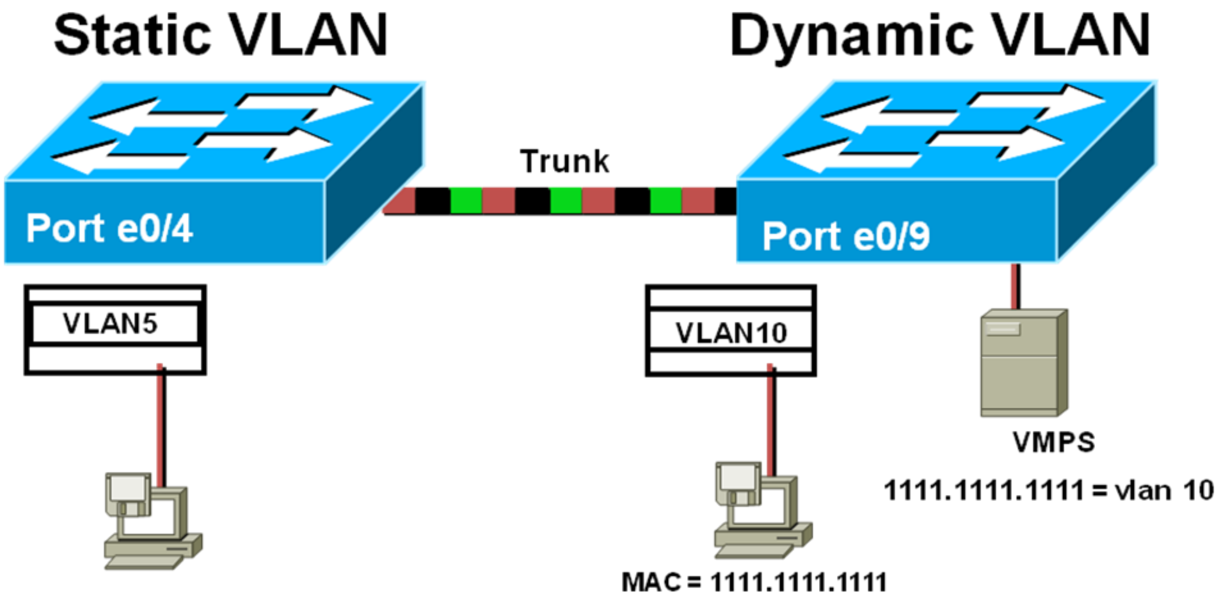
*Each logical VLAN is like a separate physical bridge
*VLANs can span across multiple switches

VLAN Operations



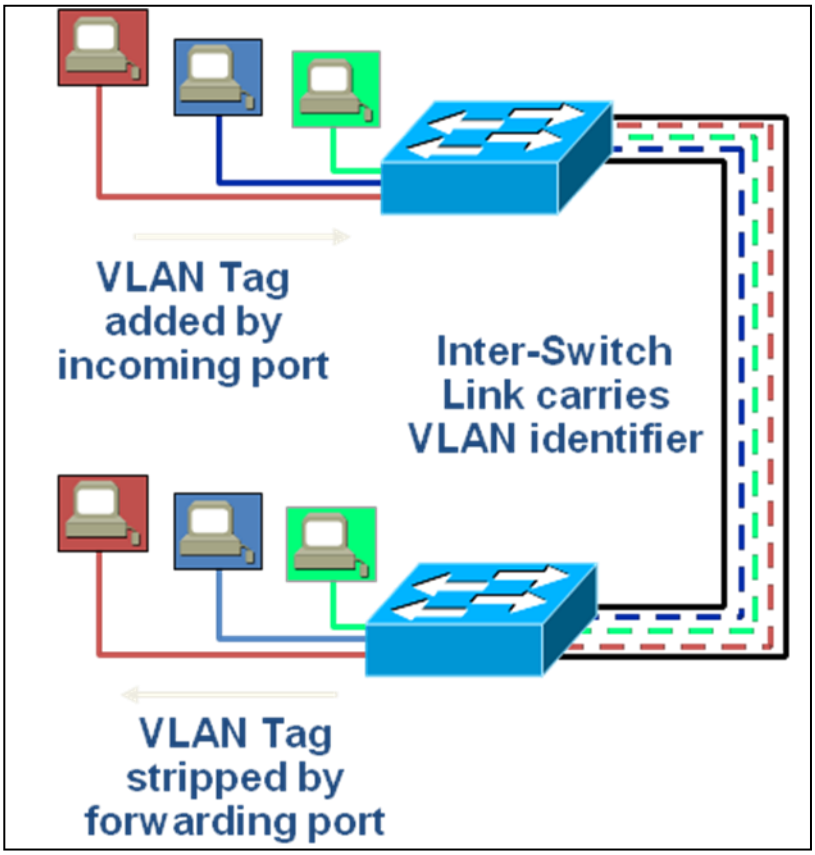
*Each logical VLAN is like a separate physical bridge
*VLANs can span across multiple switches
*Trunks carries traffic for multiple VLANs

VLAN Membership Modes



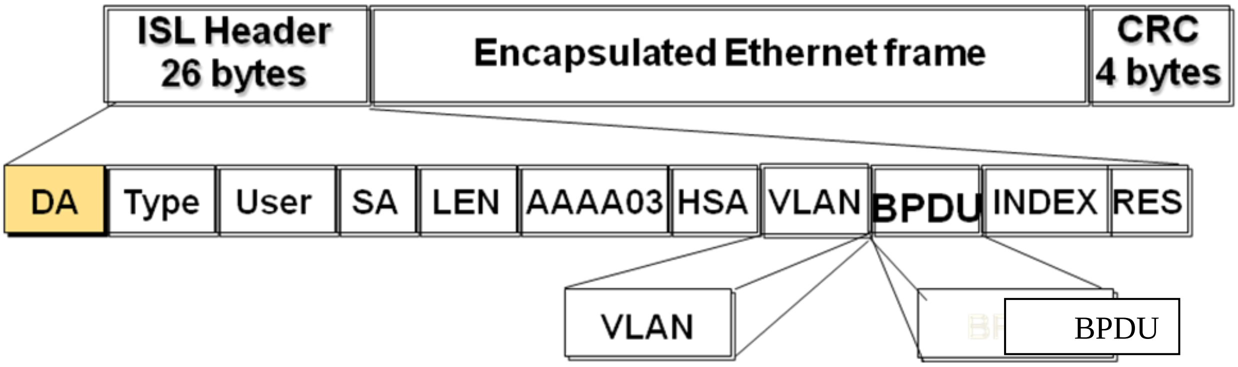
ISL Tagging

ISL trunks enable VLANs across a backbone



*Performed with ASIC
*Not intrusive to client stations, client does not see the ISL header
*Effective between switches, routers and switches, switches and servers with ISL network interface cards

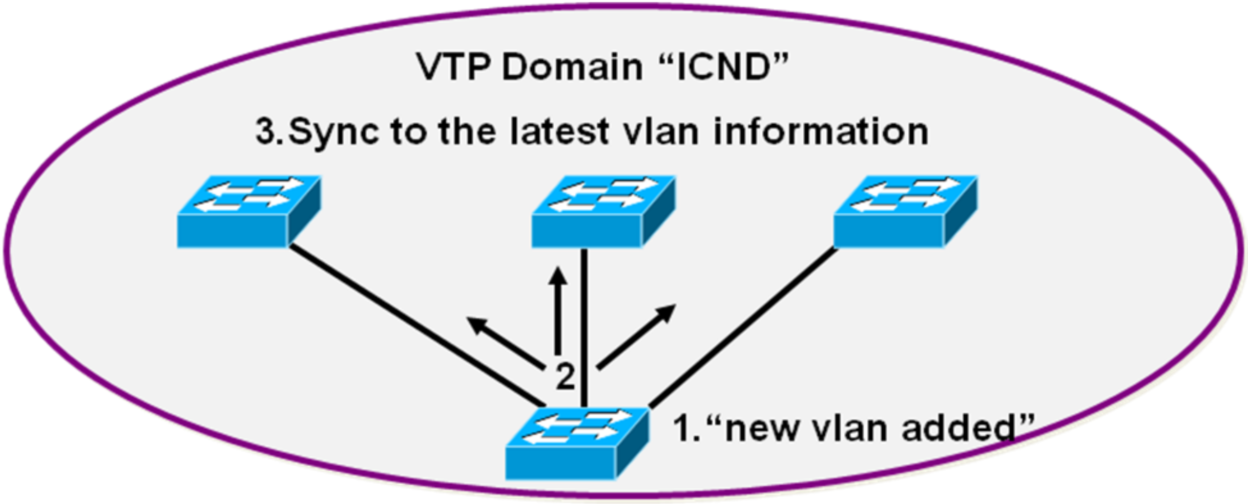
ISL Encapsulation



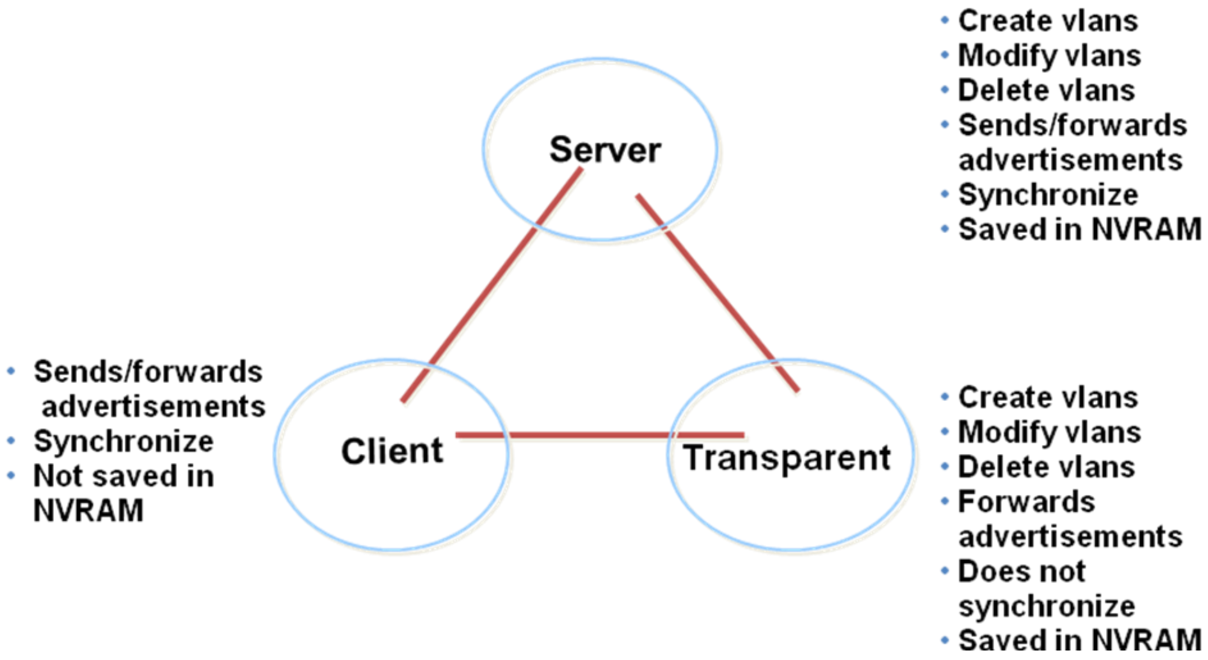
*Frames encapsulated with ISL header and CRC
*Support for many VLANs (1024)
*VLAN field
*BPDU bit

VLAN Trunking Protocol (VTP)

*A messaging system that advertises VLAN configuration information
*Maintains VLAN configuration consistency throughout a common **administrative domain**
*VTP sends advertisements on trunk ports only
*Support mixed media trunks (Fast Ethernet, FDDI, ATM)



VTP Modes



- Create vlans
- Modify vlans
- Delete vlans
- Sends/forwards advertisements
- Synchronize
- Saved in NVRAM

- Sends/forwards advertisements
- Synchronize
- Not saved in NVRAM

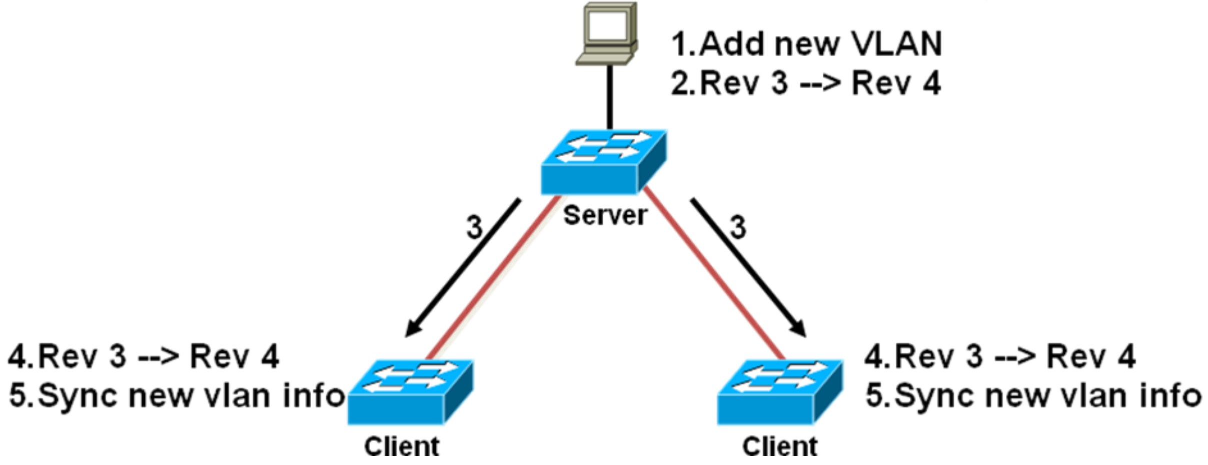
- Create vlans
- Modify vlans
- Delete vlans
- Forwards advertisements
- Does not synchronize
- Saved in NVRAM

How VTP Works

*VTP advertisements are sent as multicast frames
*VTP servers and clients synchronized to latest revision number
*VTP advertisement are sent every five minutes or when there is a change

How VTP Works

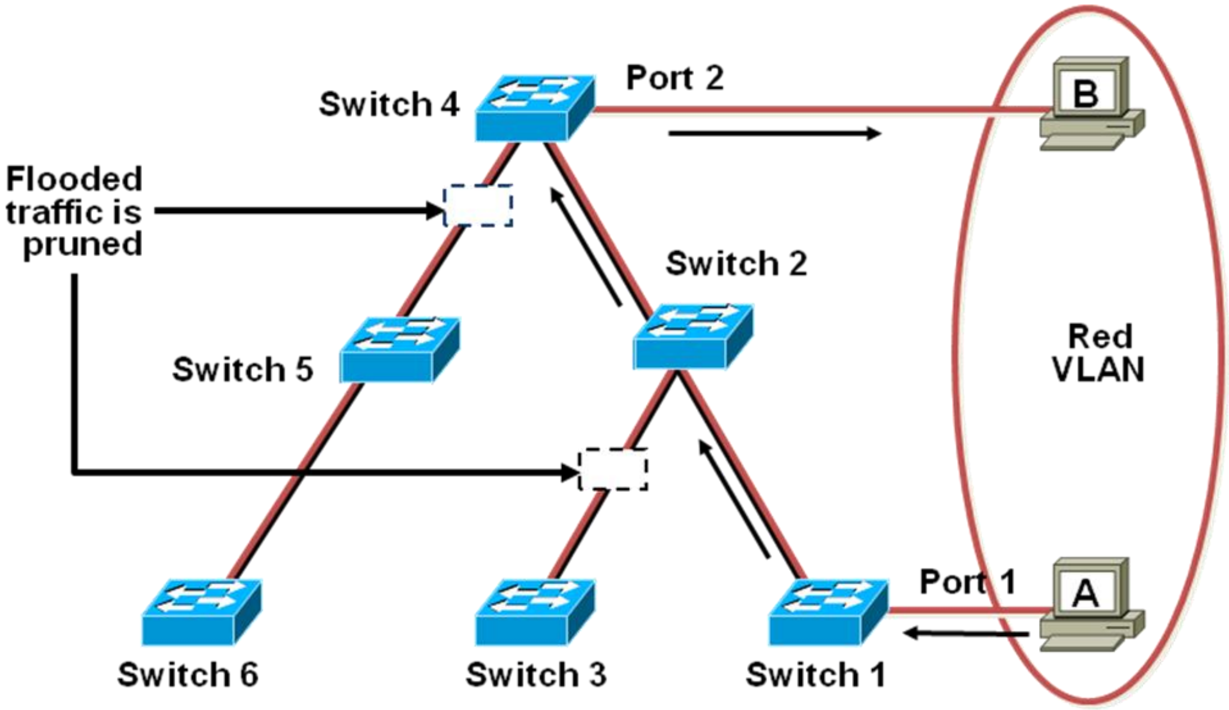
*VTP advertisements are sent as multicast frames
*VTP servers and clients synchronized to latest revision number
*VTP advertisement are sent every five minutes or when there is a change



VTP Pruning

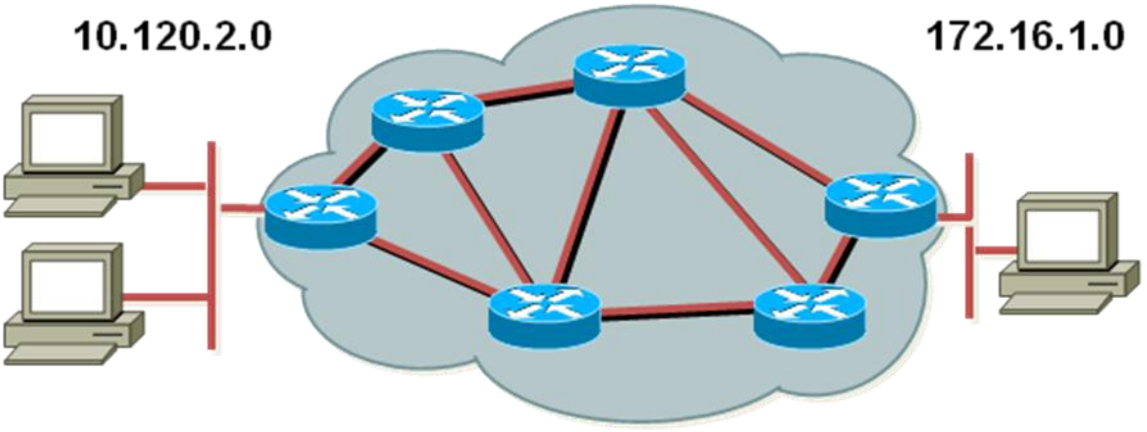
*Increases available bandwidth by reducing unnecessary flooded traffic
*Example: Station A sends broadcast, broadcast is only flooded toward any **switch with ports**

assigned to the red VLAN



Routing

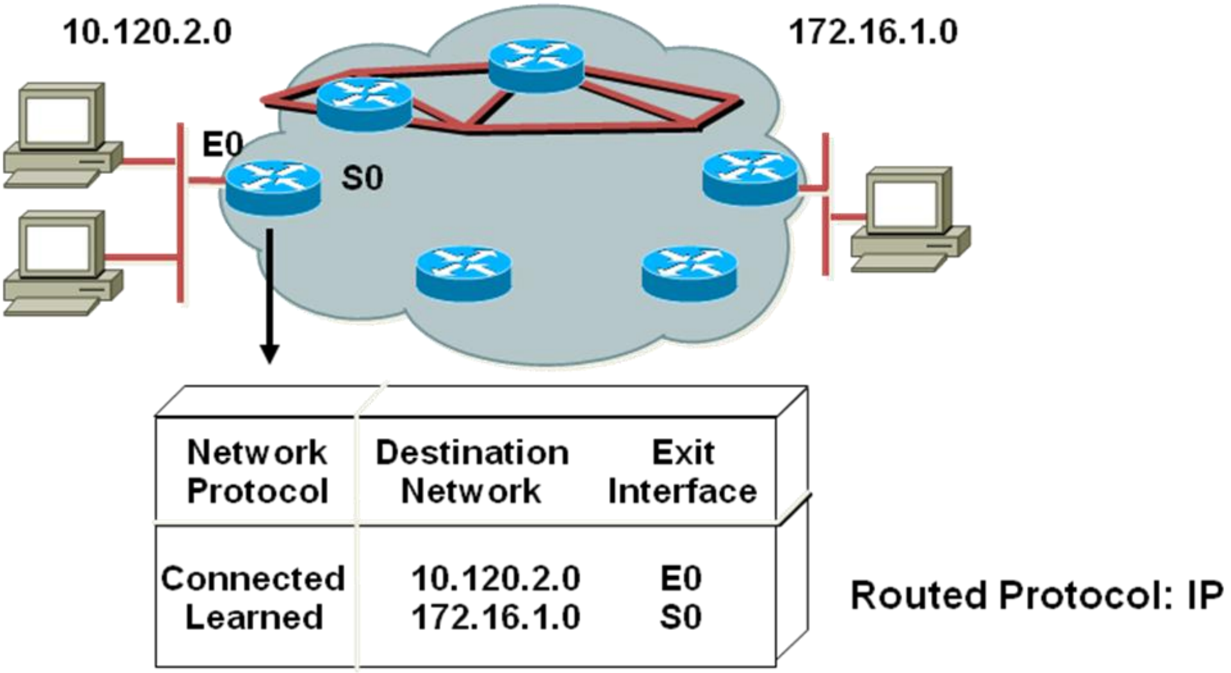
What is Routing?



To route a router need to know:

*Destination addresses
*Sources it can learn from
*Possible routes
*Best route
*Maintain and verify routing information

What is Routing? (cont.)



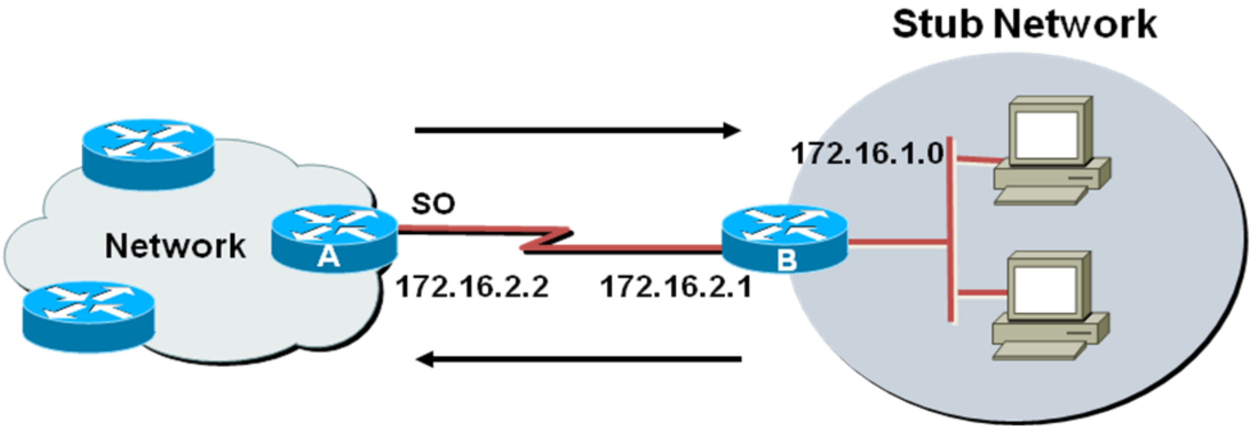
Network Protocol	Destination Network	Exit Interface
Connected Learned	10.120.2.0 172.16.1.0	E0 S0

Routers must learn destinations that are not directly connected

Identifying Static and Dynamic Routes

Static Route	Dynamic Route
Uses a route that a network administrator enters into the router manually	Uses a route that a network routing protocol adjusts automatically for topology or traffic changes

Static Routes

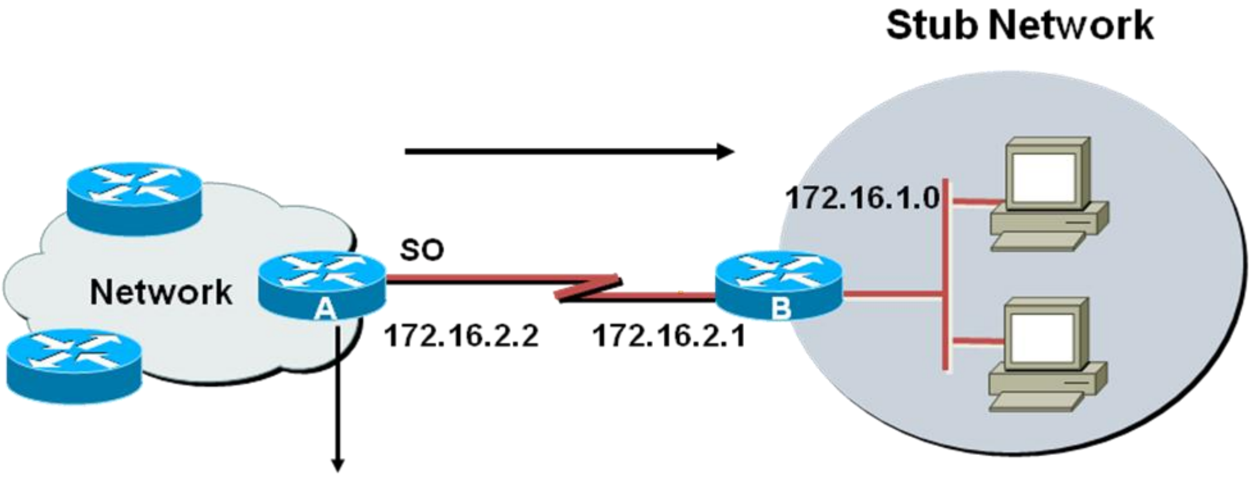


Configure unidirectional static routes to and from a stub network to allow communications to occur.

Static Route Configuration

MONA(config)#ip route network [mask]
{address | interface}[distance] [permanent]
Defines a path to an IP destination network or subnet

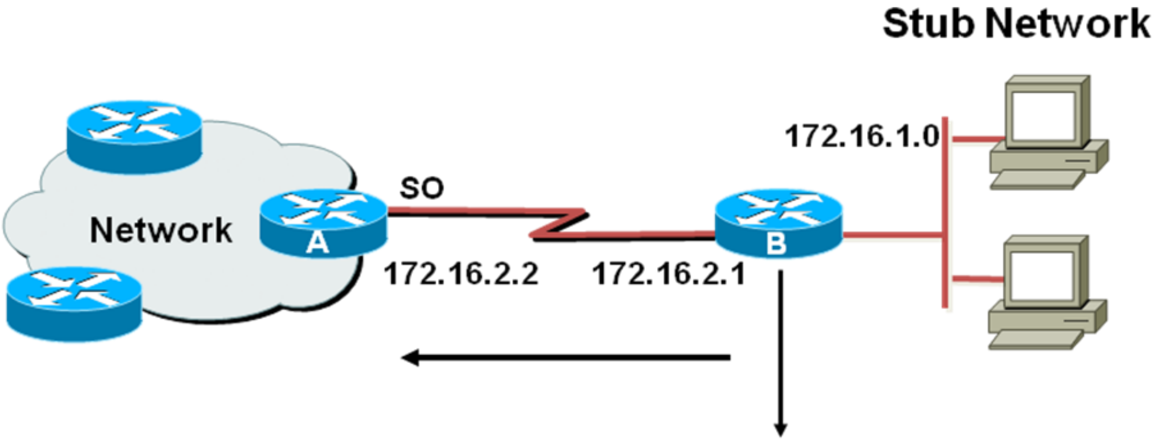
Static Route Example



```
ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

This is a unidirectional route. You must have a route configured in the opposite direction.

Default Routes



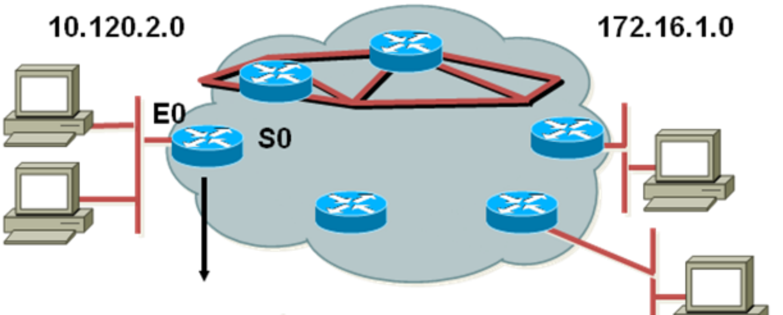
```
ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

This route allows the stub network to reach all known networks beyond router A.

What is a Routing Protocol?

Routing protocols are used between routers to determine paths and maintain routing tables.

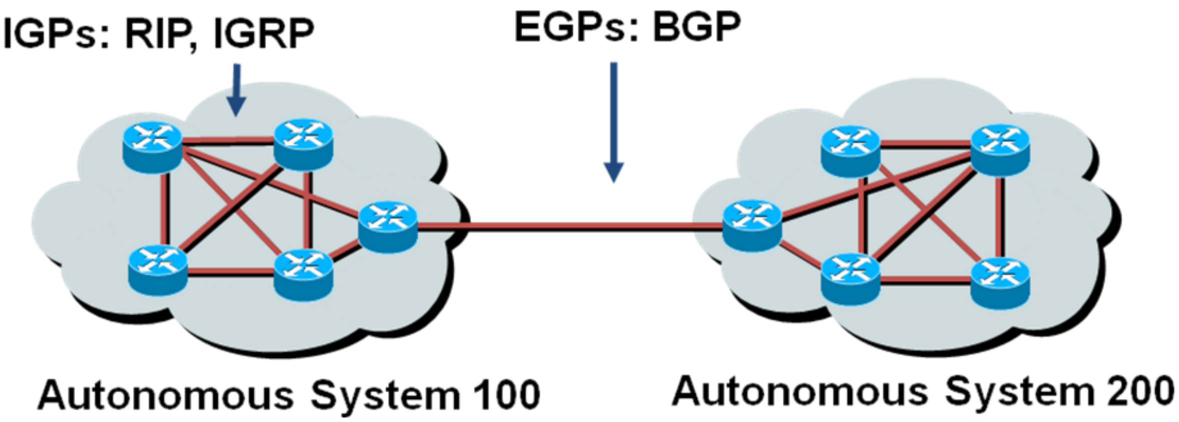
Once the path is determined a router can route a routed protocol.



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.17.3.0	S1

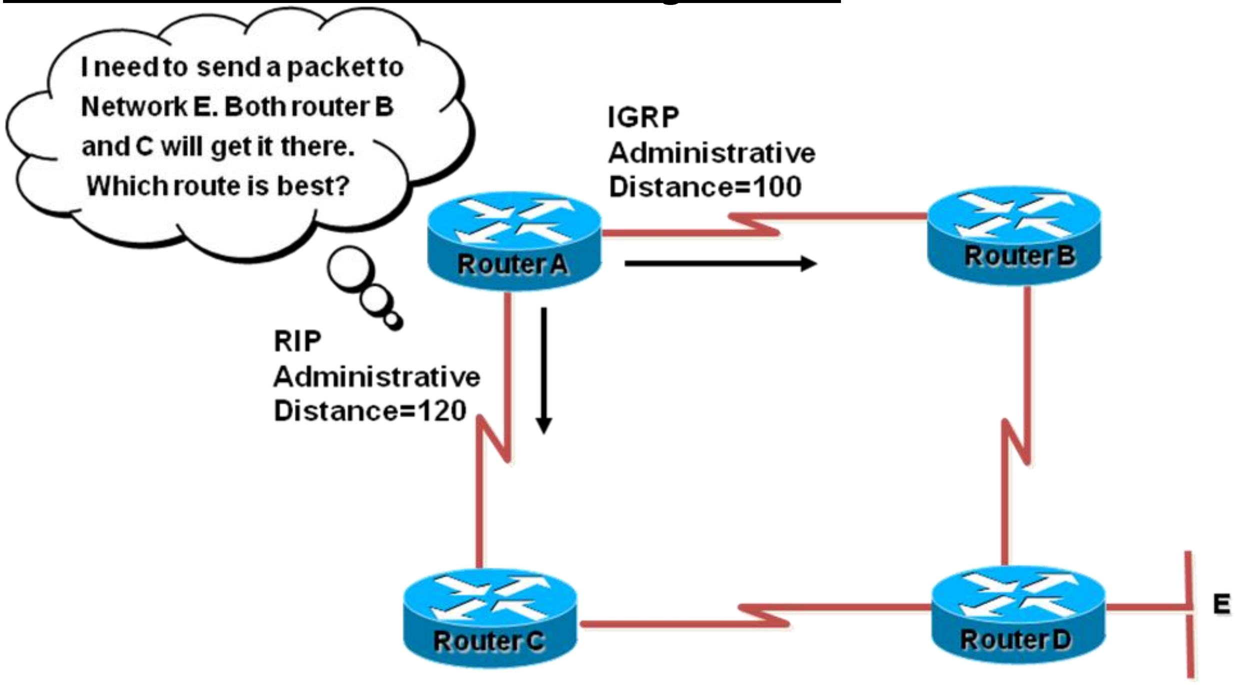
Routed Protocol: IP
Routing protocol: RIP, IGRP

Autonomous Systems: Interior or Exterior Routing Protocols



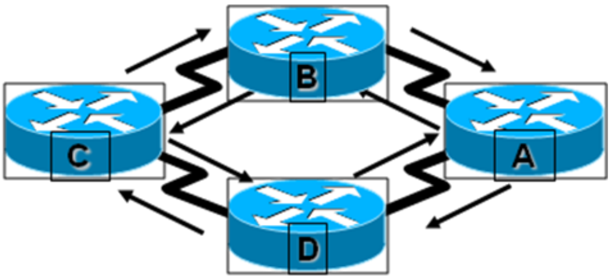
*An autonomous system is a collection of networks under a common administrative domain
*IGPs operate within an autonomous system
*EGPs connect different autonomous systems

Administrative Distance: Ranking Routes

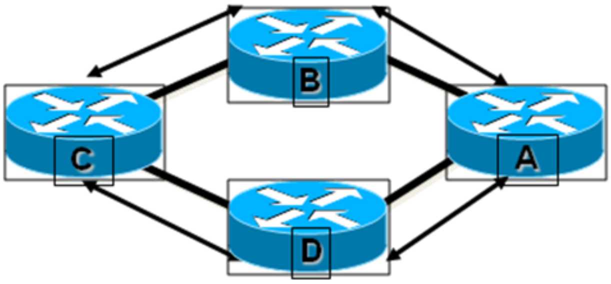

I need to send a packet to Network E. Both router B and C will get it there. Which route is best?
IGRP Administrative Distance=100
RIP Administrative Distance=120
Router A
Router B
Router C
Router D
E

Classes of Routing Protocols

Distance Vector

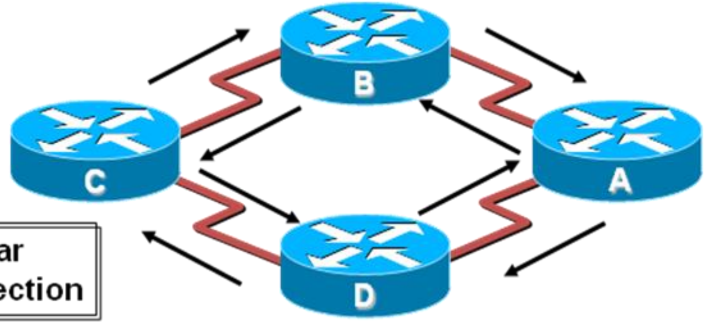


Hybrid Routing

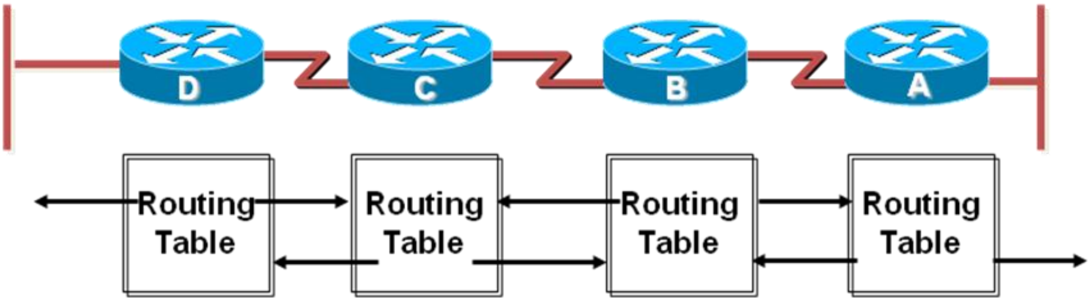


Link State

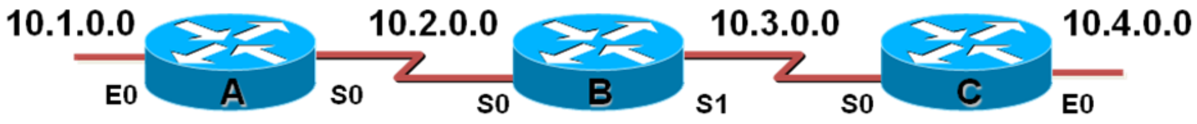
Distance Vector Routing Protocols



Distance—How far
Vector—In which direction



Distance Vector—Sources of Information and Discovering Routes

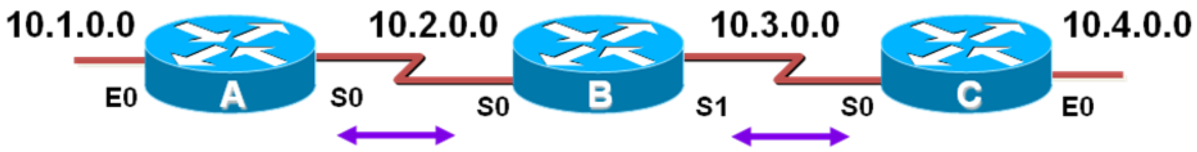


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0

Distance Vector—Sources of Information and Discovering Routes



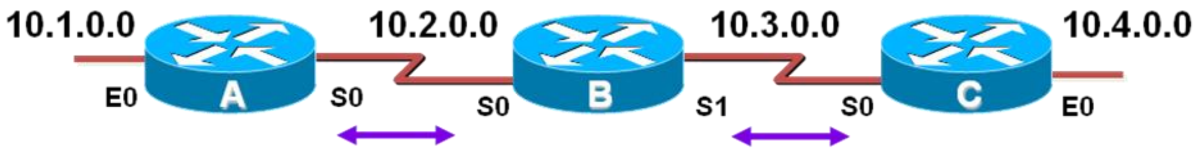
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1

Routers discover the best path to destinations from each neighbor

Distance Vector—Sources of Information and Discovering Routes



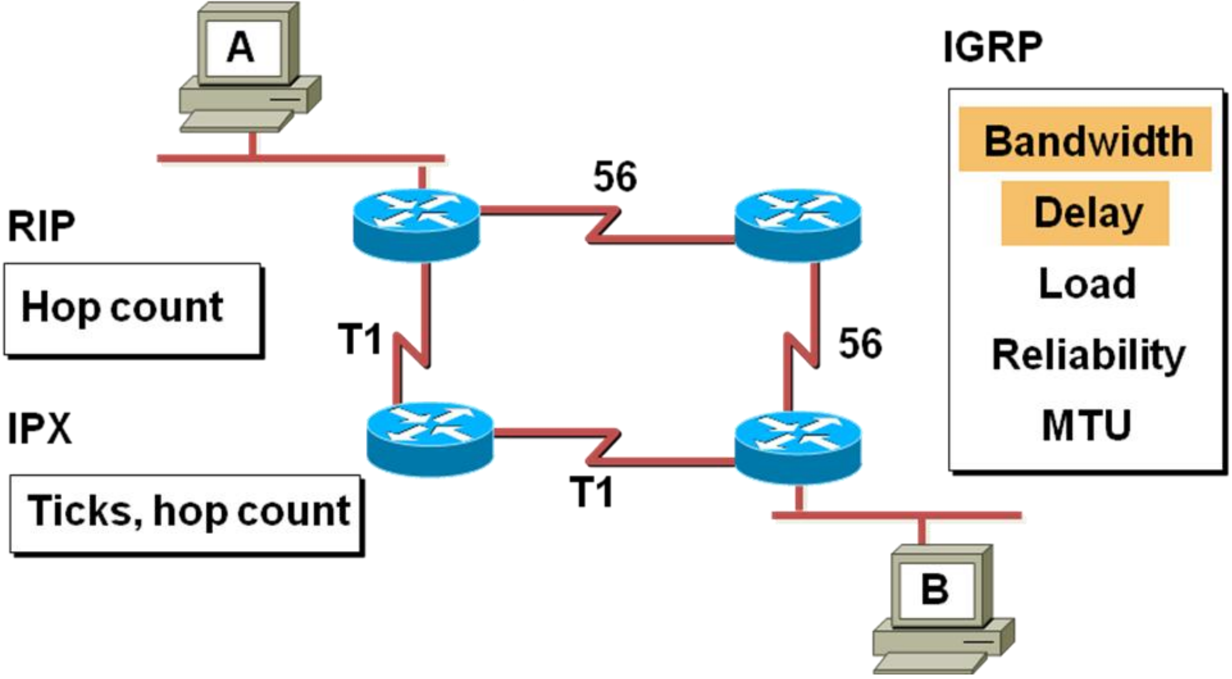
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Routers discover the best path todestinations from each neighbor

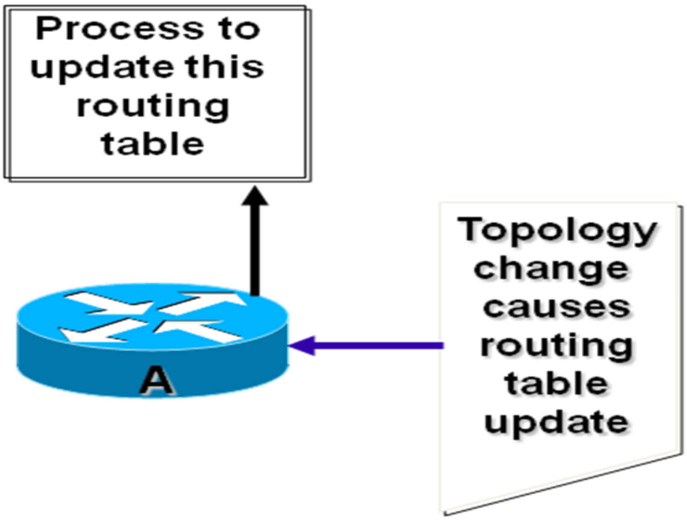
Distance Vector—Selecting Best Route with Metrics



Distance Vector—Maintaining Routing Information

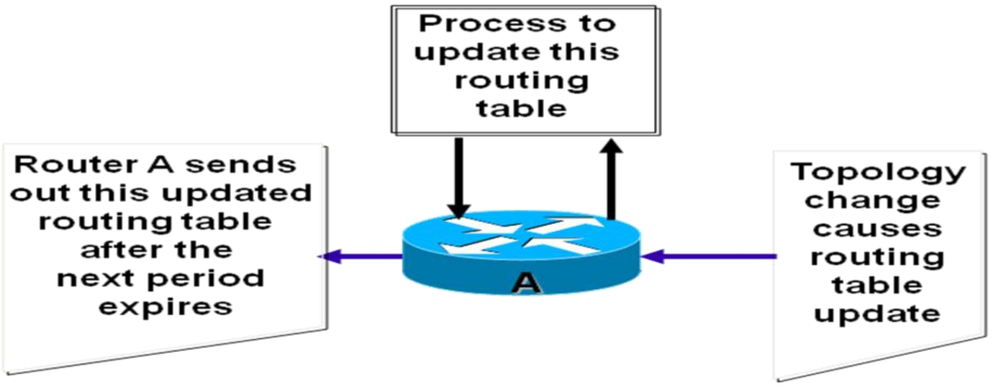
Updates proceed step-by-step

from router to router



Process to update this routing table
A
Topology change causes routing table update

Distance Vector—Maintaining Routing Information



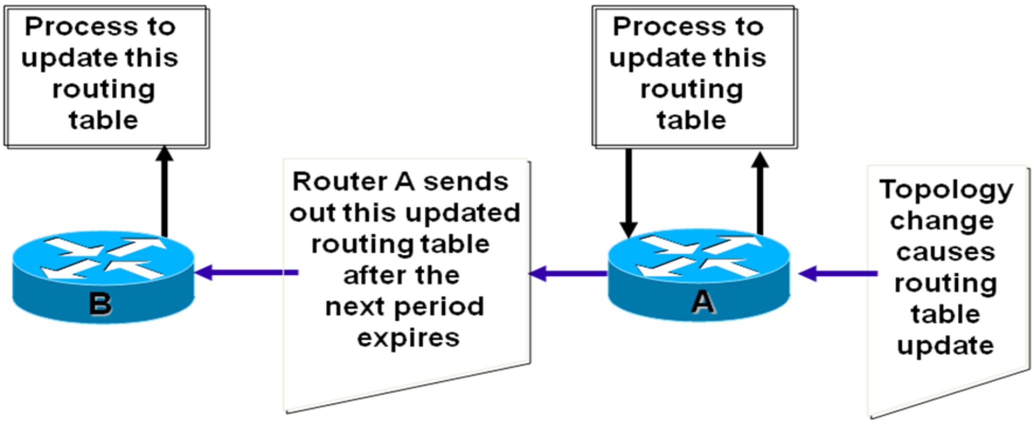
Process to update this routing table

Router A sends out this updated routing table after the next period expires

Topology change causes routing table update

Updates proceed step-by-step from router to router

Distance Vector—Maintaining Routing Information



Process to update this routing table

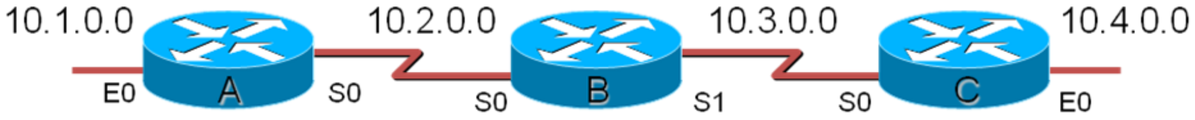
Process to update this routing table

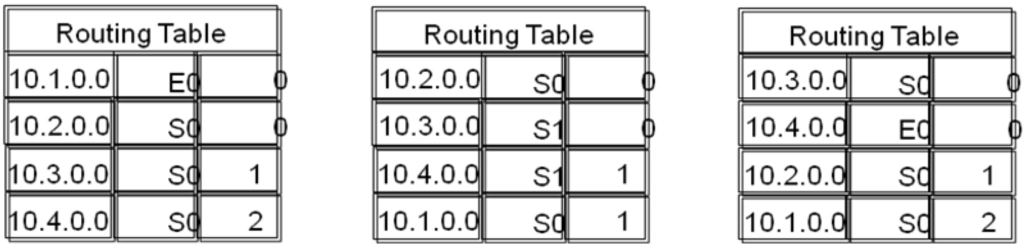
Router A sends out this updated routing table after the next period expires

Topology change causes routing table update

Updates proceed step-by-step from router to router

Maintaining Routing Information Problem—Routing Loops





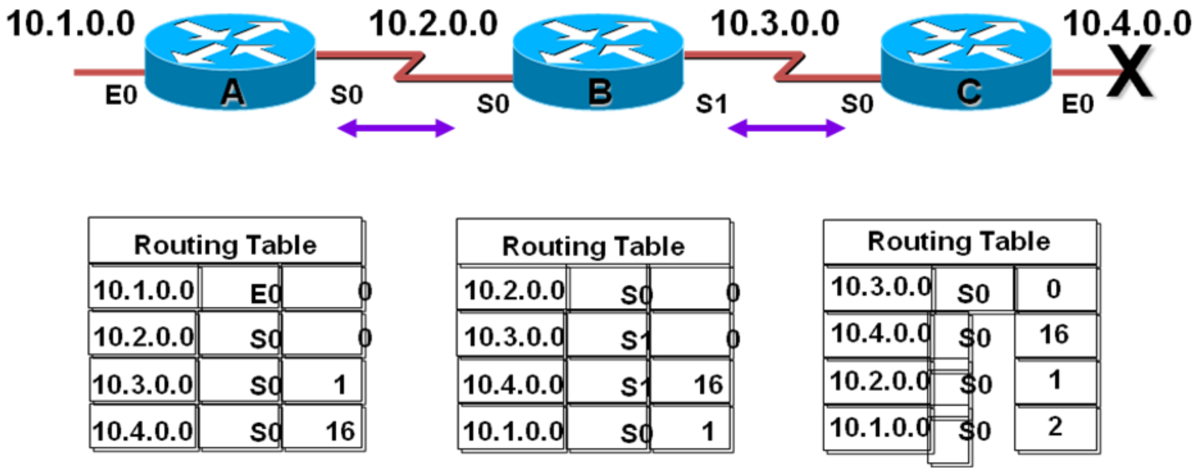
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Each node maintains the distance from itself to each possible destination network

Defining a Maximum

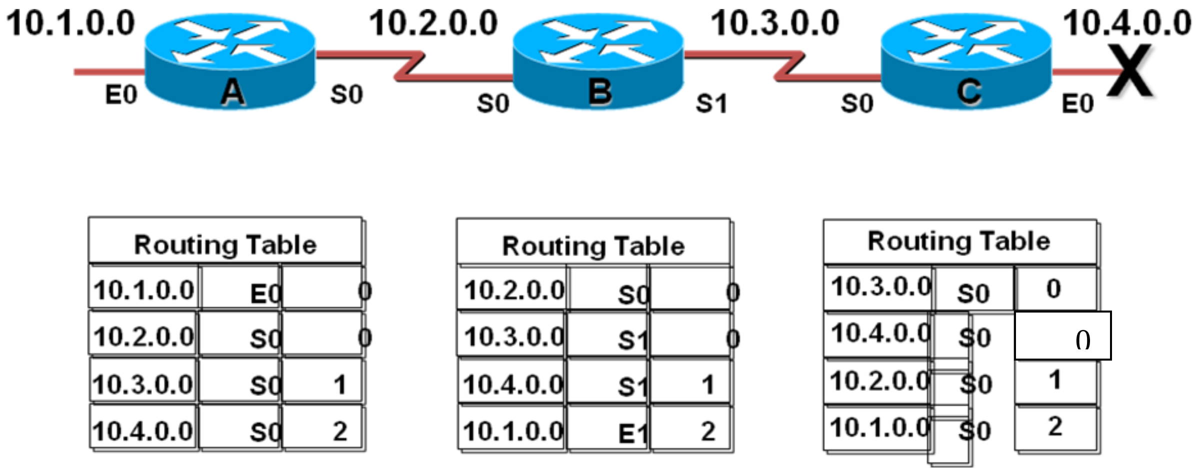


Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	16

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	16
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	16
10.2.0.0	S0	1
10.1.0.0	S0	2

Split Horizon



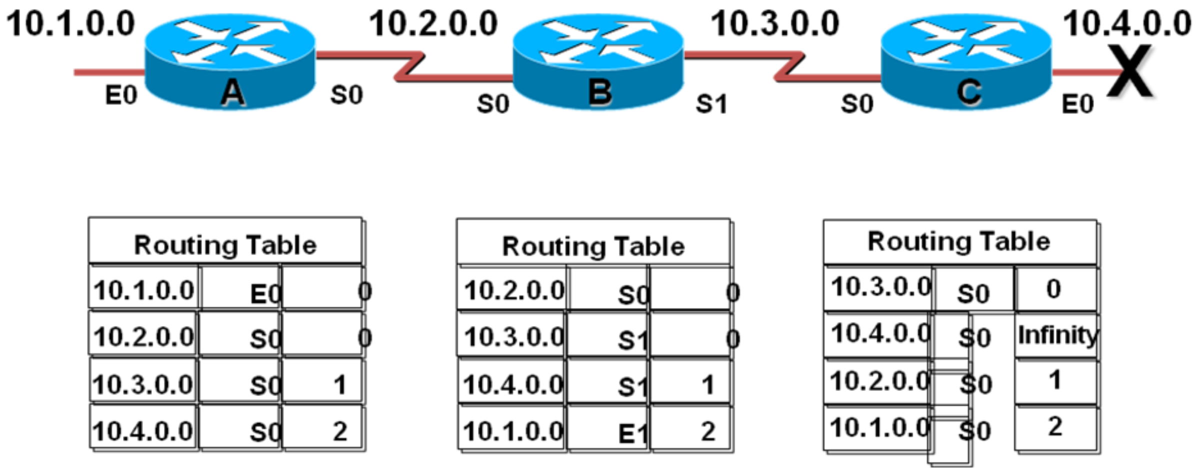
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	E1	2

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

It is never useful to send information about a route back in the direction from which the original packet came

Solution: Route Poisoning



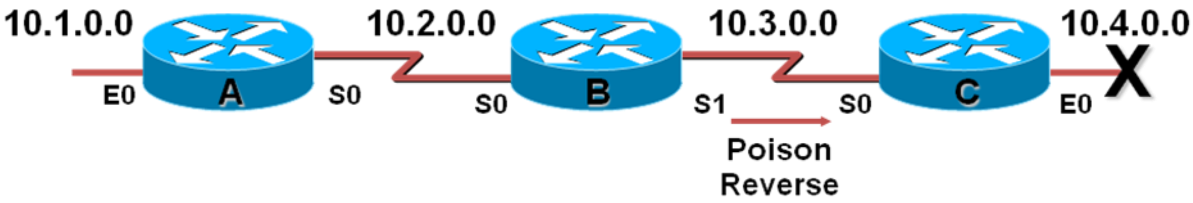
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	E1	2

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	Infinity
10.2.0.0	S0	1
10.1.0.0	S0	2

Routers set the distance of routes that have gone down to infinity

Poison Reverse



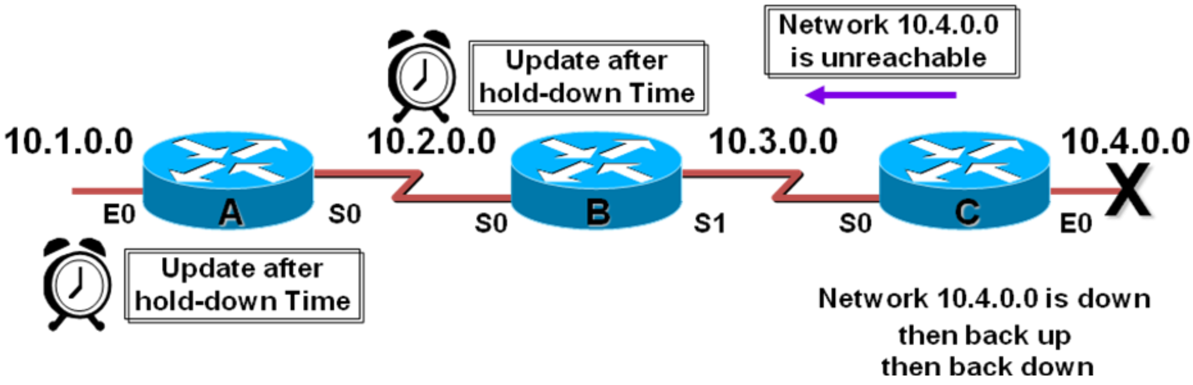
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	Possibly Down
10.1.0.0	E1	2

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	Infinity
10.2.0.0	S0	1
10.1.0.0	S0	2

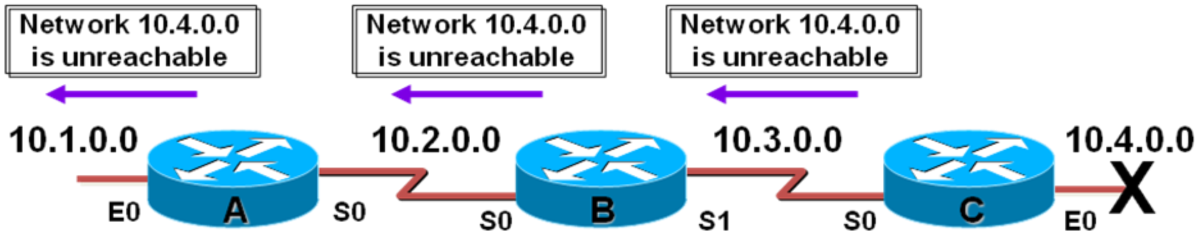
Poison Reverse overrides split horizon

Hold-Down Timers



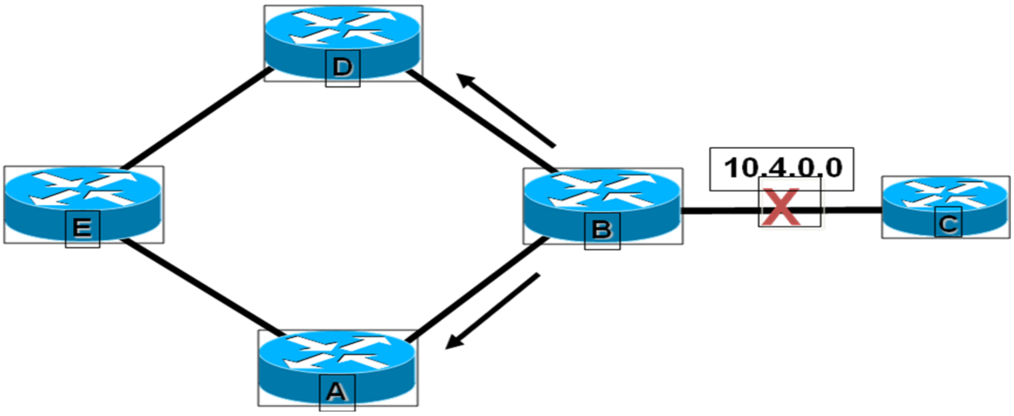
Router keeps an entry for the network possibly down state, allowing time for other routers to recompute for this topology change

Triggered Updates

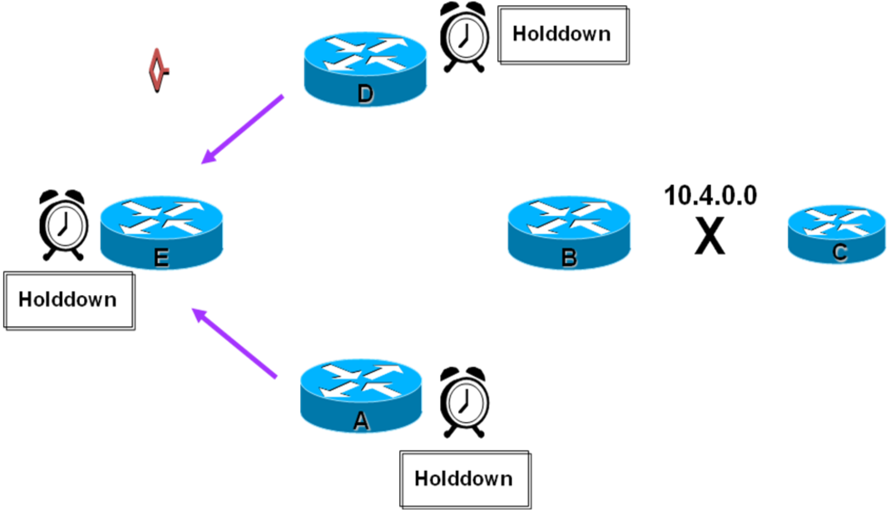


Router sends updates when a change in its routing table occurs

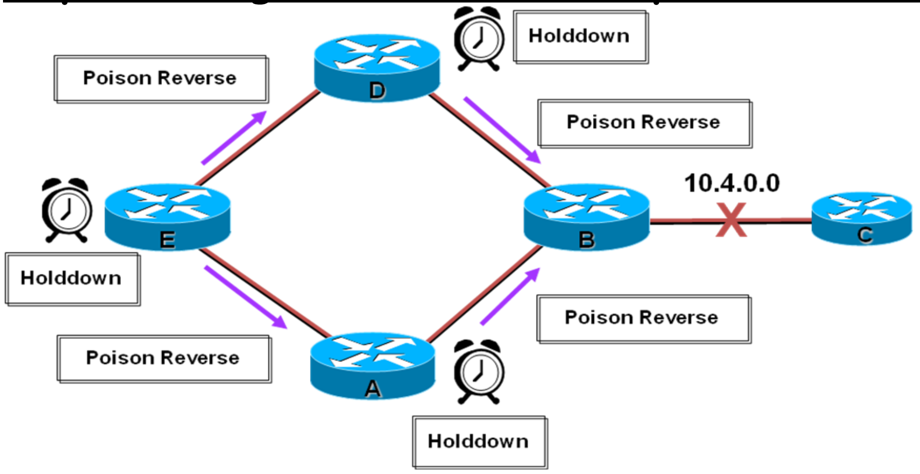
Implementing Solutions in Multiple Routes



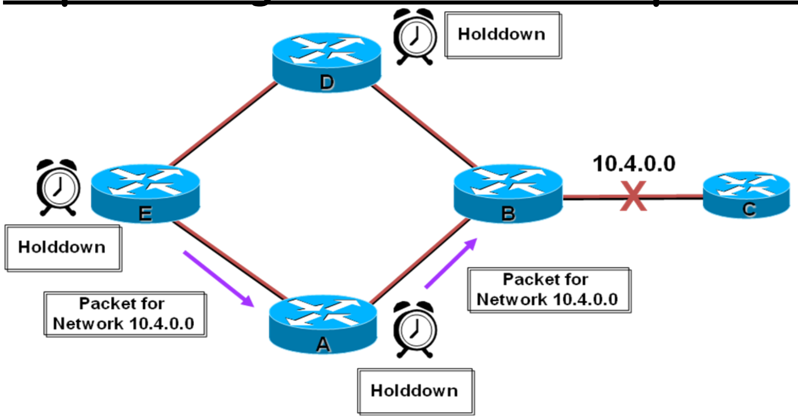
Implementing Solutions in Multiple Routes (cont.)



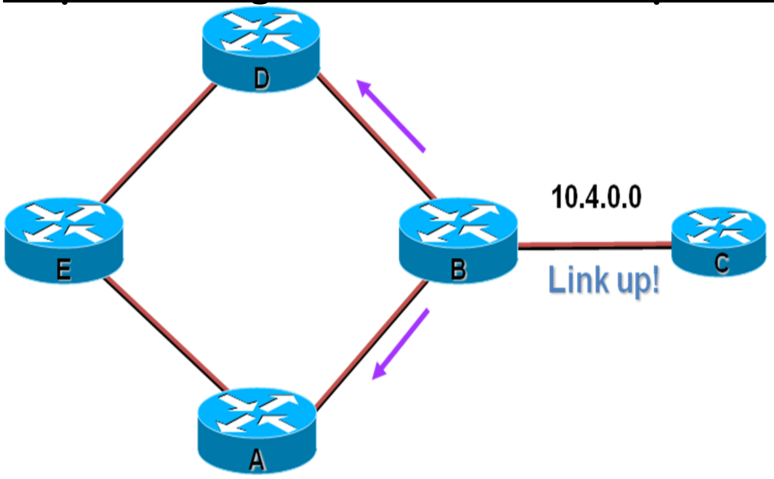
Implementing Solutions in Multiple Routes (cont.)



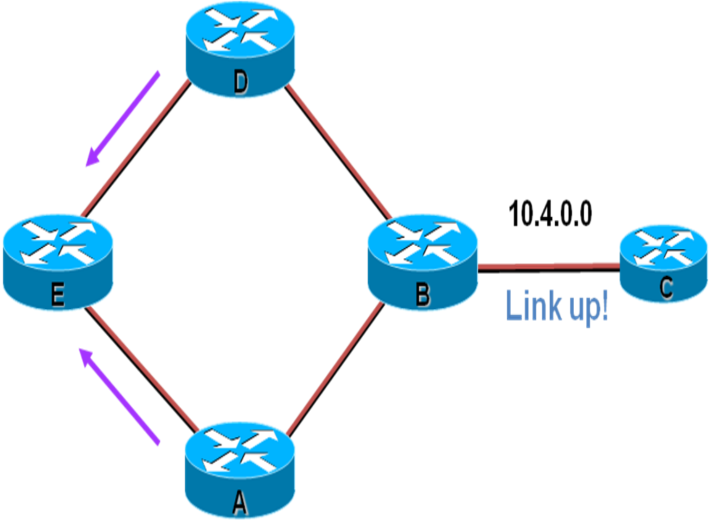
Implementing Solutions in Multiple Routes (cont.)



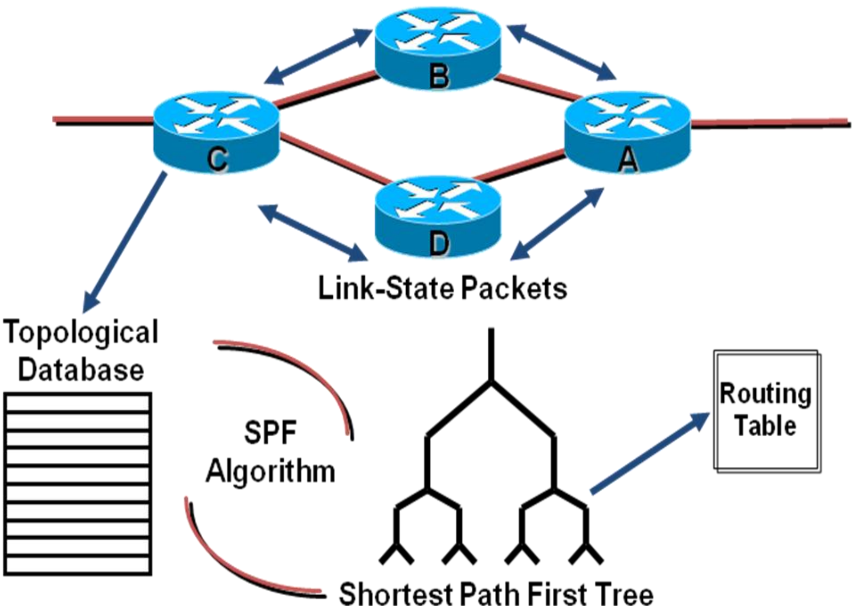
Implementing Solutions in Multiple Routes (cont.)



Implementing Solutions in Multiple Routes (cont.)

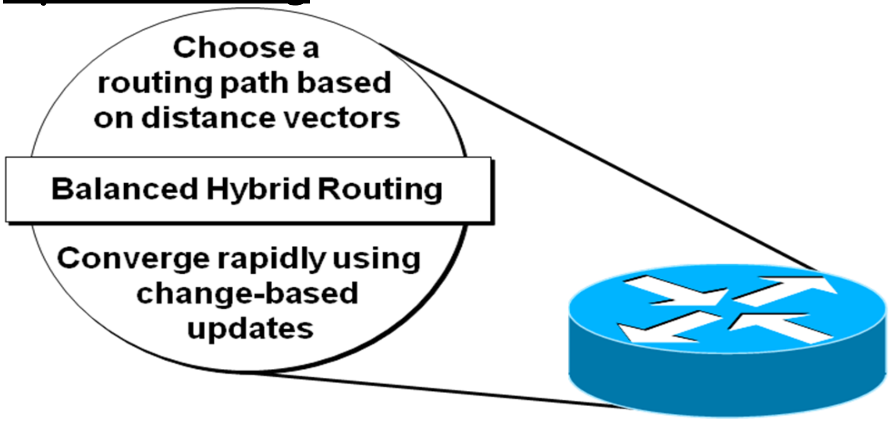


Link-State Routing Protocols



After initial flood, pass small event-triggered link-state updates to all other routers

Hybrid Routing


Choose a routing path based on distance vectors
Balanced Hybrid Routing
Converge rapidly using change-based updates

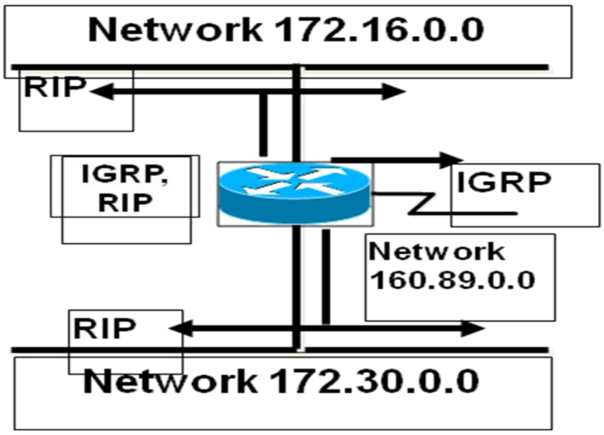
Share attributes of both distance-vector and link-state routing

IP Routing Configuration Tasks

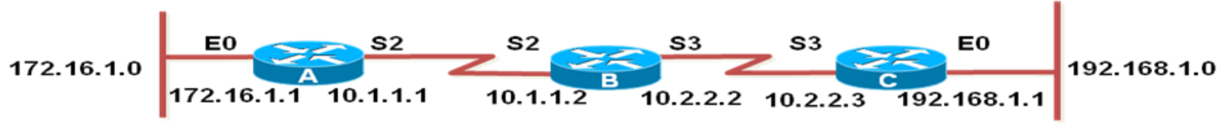
Router configuration

*Select routing protocols

*Specify networks or interfaces



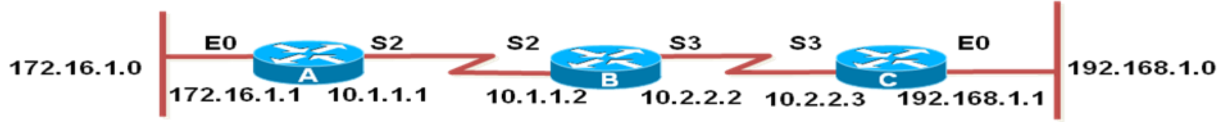
Verifying the Routing Protocol—RIP



MONA-A#sh ip protocols

```
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface        Send  Recv   Key-chain
    Ethernet0         1     1 2
    Serial2           1     1 2
  Routing for Networks:
    10.0.0.0
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2           120      00:00:10
  Distance: (default is 120)
```

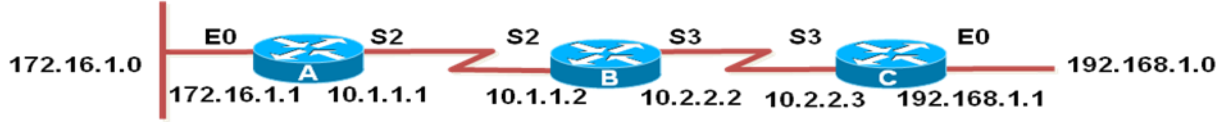
Displaying the IP Routing Table



MONA-A#sh ip route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Ethernet0
     10.0.0.0/24 is subnetted, 2 subnets
R       10.2.2.0 [120/1] via 10.1.1.2, 00:00:07, Serial2
C       10.1.1.0 is directly connected, Serial2
R    192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:07, Serial2
```

debug ip rip Command



MONA#debug ip rip

```
RIP protocol debugging is on
```

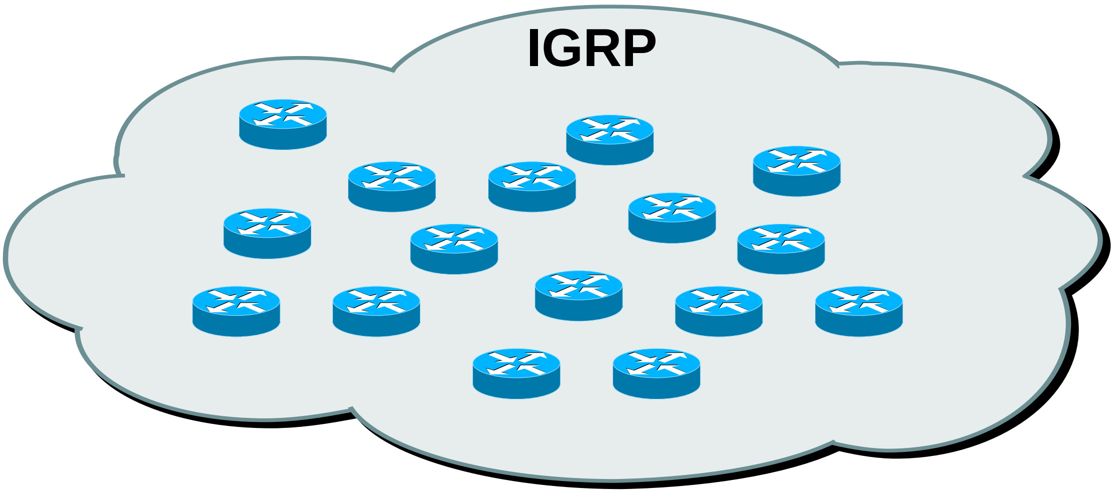
MONA-A#

```
00:06:24: RIP: received v1 update from 10.1.1.2 on Serial2
00:06:24:      10.2.2.0 in 1 hops
00:06:24:      192.168.1.0 in 2 hops
00:06:33: RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:06:34:      network 10.0.0.0, metric 1
```

```
00:06:34:      network 192.168.1.0, metric 3
00:06:34: RIP: sending v1 update to 255.255.255.255 via Serial2 (10.1.1.1)
00:06:34:      network 172.16.0.0, metric 1
```

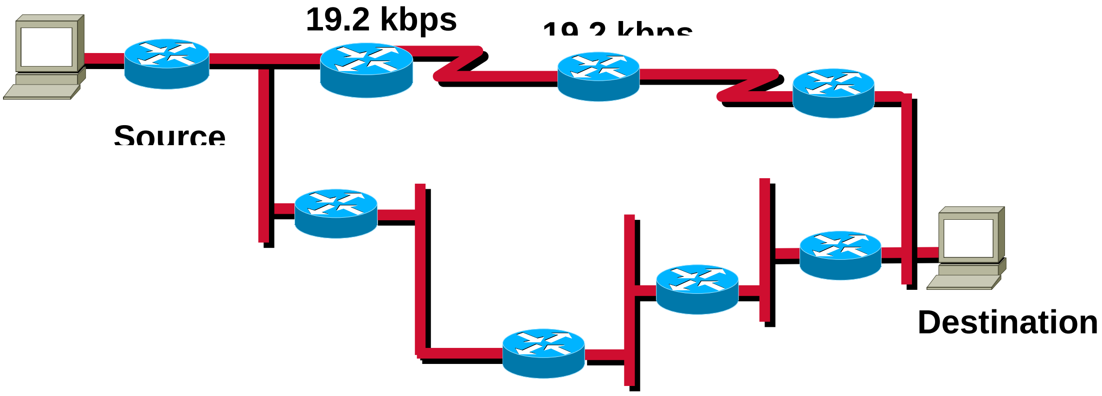
IGRP

Introduction to IGRP



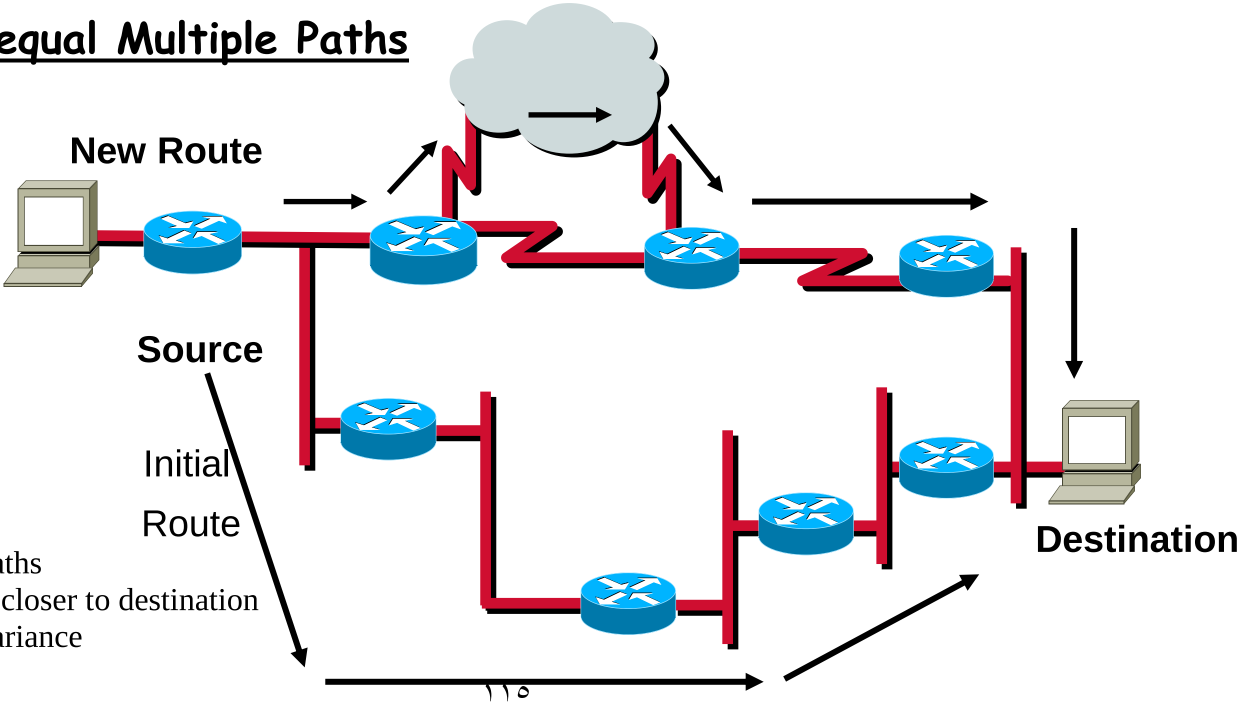
*More scalable than RIP
*Sophisticated metric
*Multiple-path support

IGRP Composite Metric



*Bandwidth
*Delay
*Reliability
*Loading
*MTU

IGRP Unequal Multiple Paths



*Maximum six paths
*Next-hop router closer to destination
*Within metric variance

Configuring IGRP

MONA(config)#router igrp *autonomous-system*

**Defines IGRP as the IP routing protocol*

MONA(config-router)#network *network-number*

**Selects participating attached networks*

Configuring IGRP (cont.)

MONA(config-router)#variance multiplier

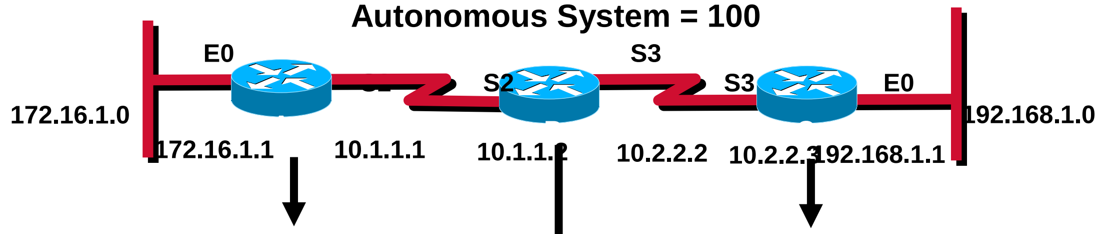
**Control IGRP load balancing*

MONA(config-router)#traffic-share { balanced | min }

**Control how load-balanced traffic is distributed*

IGRP Configuration Example

Autonomous System = 100

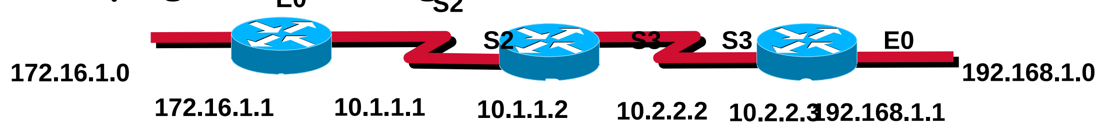


```
router igrp 100
network 172.16.0.0
network 10.0.0.0
```

```
router igrp 100
network 192.168.1.0
network 10.0.0.0
```

```
router igrp 100
network 10.0.0.0
```

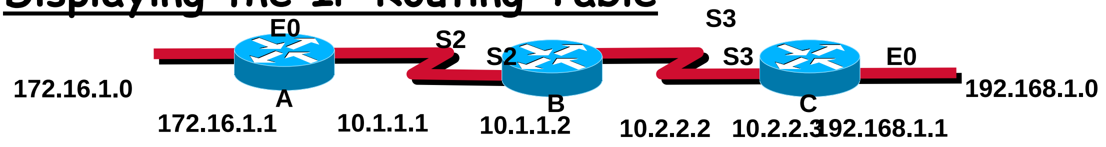
Verifying the Routing Protocol—IGRP



MONA#sh ip protocols

```
Routing Protocol is "igrp 100"
  Sending updates every 90 seconds, next due in 21 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 100
  Routing for Networks:
    10.0.0.0
    172.16.0.0
  Routing Information Sources:
    Gateway        Distance      Last Update
    10.1.1.2          100      00:01:01
  Distance: (default is 100)
```

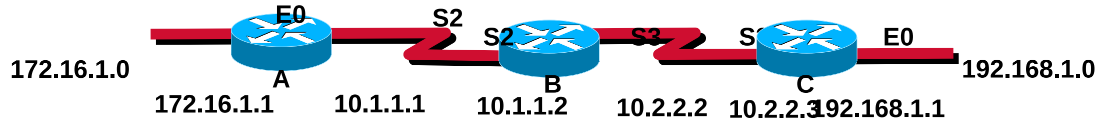
Displaying the IP Routing Table



MONA#sh ip route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Ethernet0
     10.0.0.0/24 is subnetted, 2 subnets
I       10.2.2.0 [100/90956] via 10.1.1.2, 00:00:23, Serial2
C       10.1.1.0 is directly connected, Serial2
I    192.168.1.0/24 [100/91056] via 10.1.1.2, 00:00:23, Serial2
```

debug ip igrp transaction Command



MONA#debug ip igrp transactions

```
IGRP protocol debugging is on
RouterA#
00:21:06: IGRP: sending update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:21:06:       network 10.0.0.0, metric=88956
00:21:06:       network 192.168.1.0, metric=91056
00:21:07: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:21:07:       network 172.16.0.0, metric=1100
00:21:16: IGRP: received update from 10.1.1.2 on Serial2
00:21:16:       subnet 10.2.2.0, metric 90956 (neighbor 88956)
00:21:16:       network 192.168.1.0, metric 91056 (neighbor 89056)
```

debug ip igrp events Command

MONA#debug ip igrp events
IGRP event debugging is on
MONAA#

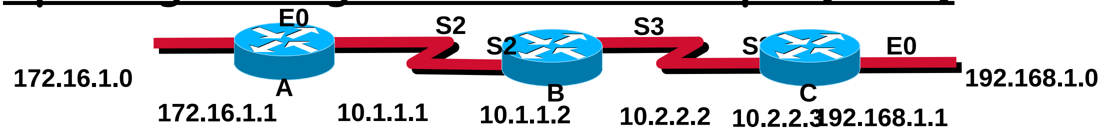
```
00:23:44: IGRP: sending update to 255.255.255.255 via Ethernet0 (172.16.1.1)
00:23:44: IGRP: Update contains 0 interior, 2 system, and 0 exterior routes.
00:23:44: IGRP: Total routes in update: 2
00:23:44: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:23:45: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:23:45: IGRP: Total routes in update: 1
00:23:48: IGRP: received update from 10.1.1.2 on Serial2
00:23:48: IGRP: Update contains 1 interior, 1 system, and 0 exterior routes.
00:23:48: IGRP: Total routes in update: 2
```

Updating Routing Information Example

MONA# debug ip igrp trans

```
00:31:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to down
00:31:15: IGRP: edition is now 3
00:31:15: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.1)
00:31:15:       network 172.16.0.0, metric=4294967295
00:31:16: IGRP: Update contains 0 interior, 1 system, and 0 exterior routes.
00:31:16: IGRP: Total routes in update: 1
00:31:16: IGRP: broadcasting request on Serial2
00:31:16: IGRP: received update from 10.1.1.2 on Serial2
00:31:16:       subnet 10.2.2.0, metric 90956 (neighbor 88956)
00:31:16:       network 172.16.0.0, metric 4294967295 (inaccessible)
00:31:16:       network 192.168.1.0, metric 91056 (neighbor 89056)
00:31:16: IGRP: Update contains 1 interior, 2 system, and 0 exterior routes.
00:31:16: IGRP: Total routes in update: 3
```

Updating Routing Information Example (cont.)



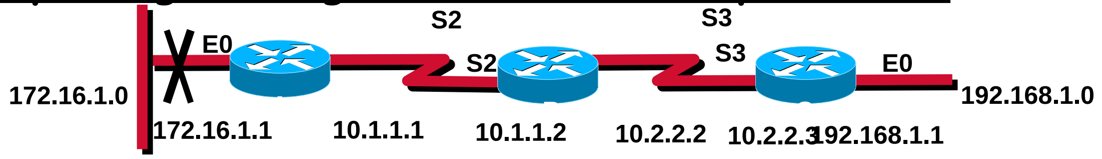
AHMED#debug ip igrp trans

IGRP protocol debugging is on

AHMEDB#

```
1d19h: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.2)
1d19h:      subnet 10.2.2.0, metric=88956
1d19h:      network 192.168.1.0, metric=89056
1d19h: IGRP: sending update to 255.255.255.255 via Serial3 (10.2.2.2)
1d19h:      subnet 10.1.1.0, metric=88956
1d19h:      network 172.16.0.0, metric=89056
1d19h: IGRP: received update from 10.1.1.1 on Serial2
1d19h:      network 172.16.0.0, metric 4294967295 (inaccessible)
1d19h: IGRP: edition is now 10
1d19h: IGRP: sending update to 255.255.255.255 via Serial2 (10.1.1.2)
1d19h:      subnet 10.2.2.0, metric=88956
1d19h:      network 172.16.0.0, metric=4294967295
1d19h:      network 192.168.1.0, metric=89056
1d19h: IGRP: sending update to 255.255.255.255 via Serial3 (10.2.2.2)
1d19h:      subnet 10.1.1.0, metric=88956
1d19h:      network 172.16.0.0, metric=4294967295
```

Updating Routing Information Example (cont.)

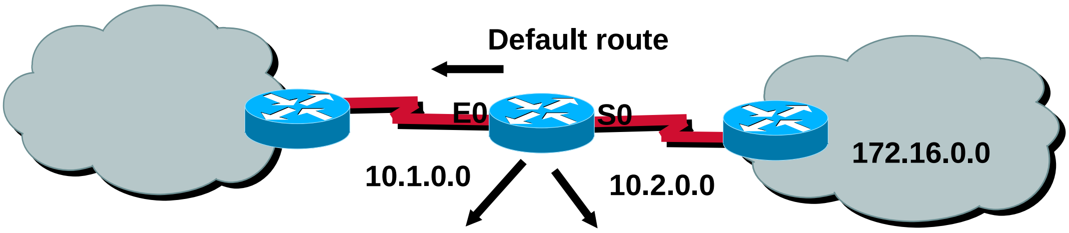


AHMED#sh ip route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route
Gateway of last resort is not set
I    172.16.0.0/16 is possibly down, routing via 10.1.1.1, Serial2
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial2
C       10.2.2.0 is directly connected, Serial3
I    192.168.1.0/24 [100/89056] via 10.2.2.3, 00:00:14, Serial3
```

```
AHMED#ping 172.16.1.1
        Type escape sequence to abort.
        Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
        Success rate is 0 percent (0/5)
AHMED#
```

ip classless Command



```
Router(config)#ip classless
```

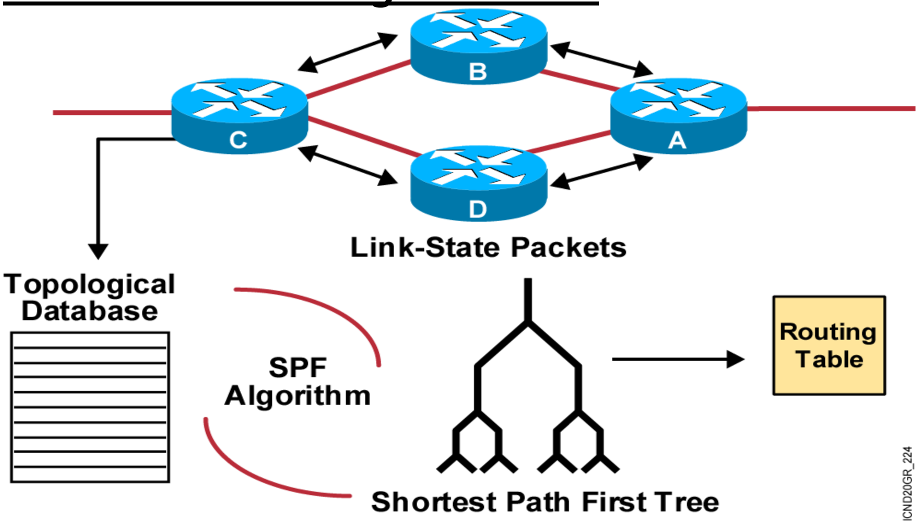
Network Protocol	Destination Network	Exit Interface
C	10.1.0.0	E0
C	10.2.0.0	S0
RIP	172.16.0.0 via	S0
	0.0.0.0	E0

To get to 10.7.1.1:

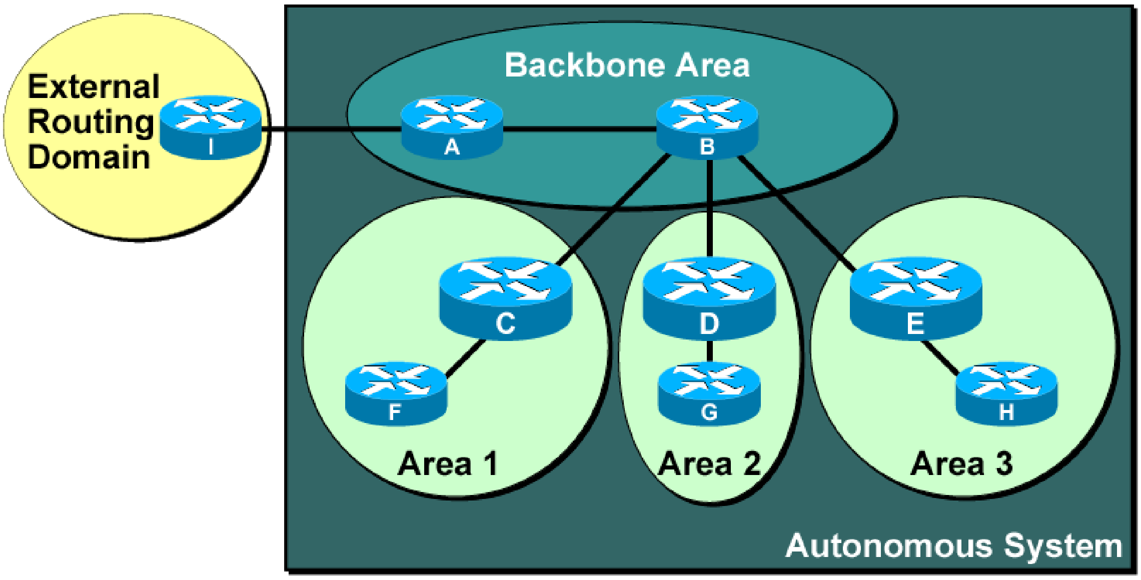
→

Link-State and Balanced Hybrid Routing

Link-State Routing Protocols

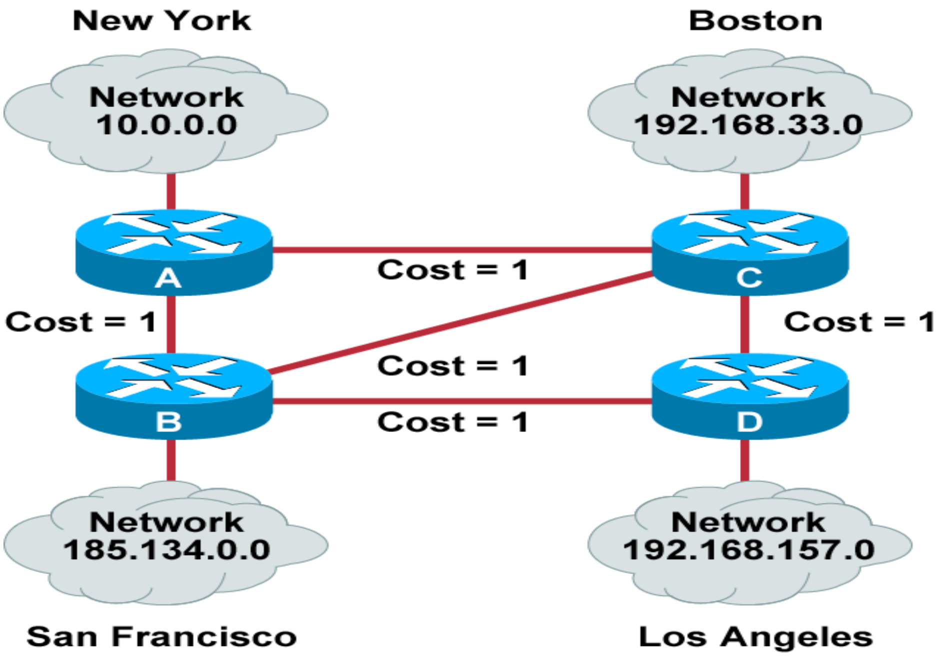


Link-State Network Hierarchy Example



*Minimizes routing table entries
*Localizes impact of a topology change within an area

Link-State Routing Protocol Algorithms



Benefits of Link-State Routing

*Fast convergence: changes are reported immediately by the source affected.
*Robustness against routing loops:
*Routers know the topology.
-Link-state packets are sequenced and acknowledged.
*By careful (hierarchical) network design, you can utilize resources optimally.

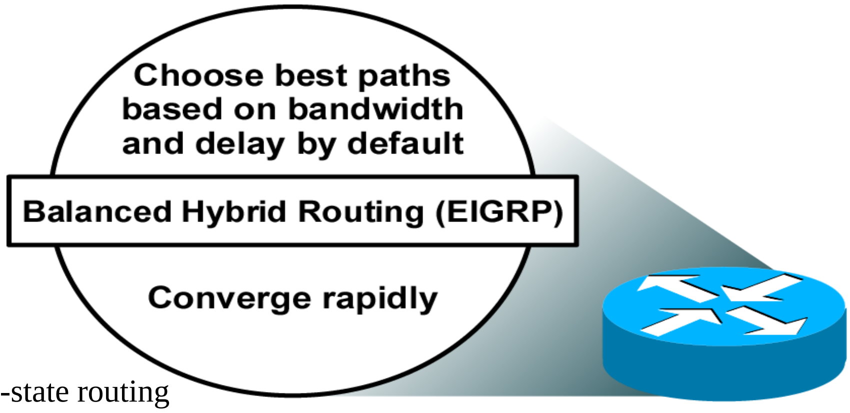
Caveats of Link-State Routing

*Significant demands for resources:
-Memory (three tables: adjacency, topology, forwarding)
-CPU (Dijkstra’s algorithm can be intensive, especially when a lot of instabilities are present.)
*Requires very strict network design (when more areas—area routing)
*Problems with partitioning of areas
*Configuration generally simple but can be complex
when tuning various parameters and when the design is complex
*Troubleshooting easier than in distance vector routing

Drawbacks to Link-State Routing Protocols

*Initial discovery may cause flooding.
*Memory- and processor-intensive.

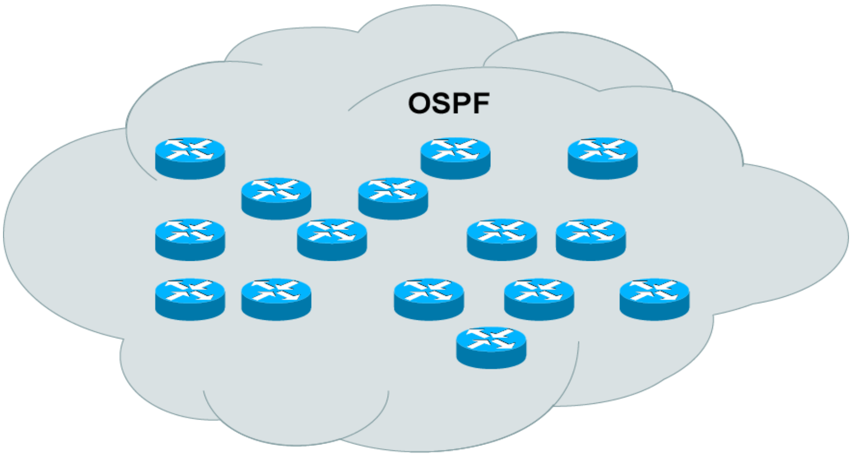
Balanced Hybrid Routing


Choose best paths based on bandwidth and delay by default
Balanced Hybrid Routing (EIGRP)
Converge rapidly

*Shares attributes of both distance vector and link-state routing

OSPF
Enabling OSPF

Introducing OSPF

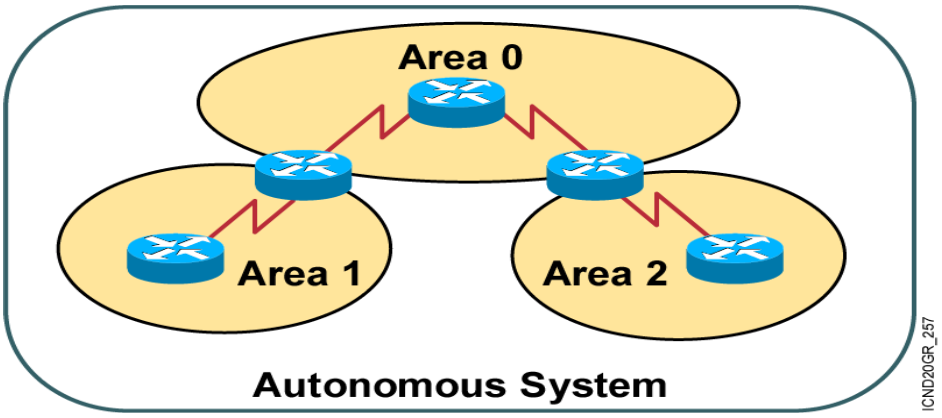


*Open standard
*Shortest path first (SPF) algorithm
*Link-state routing protocol (vs. distance vector)

OSPF as a Link-State Protocol

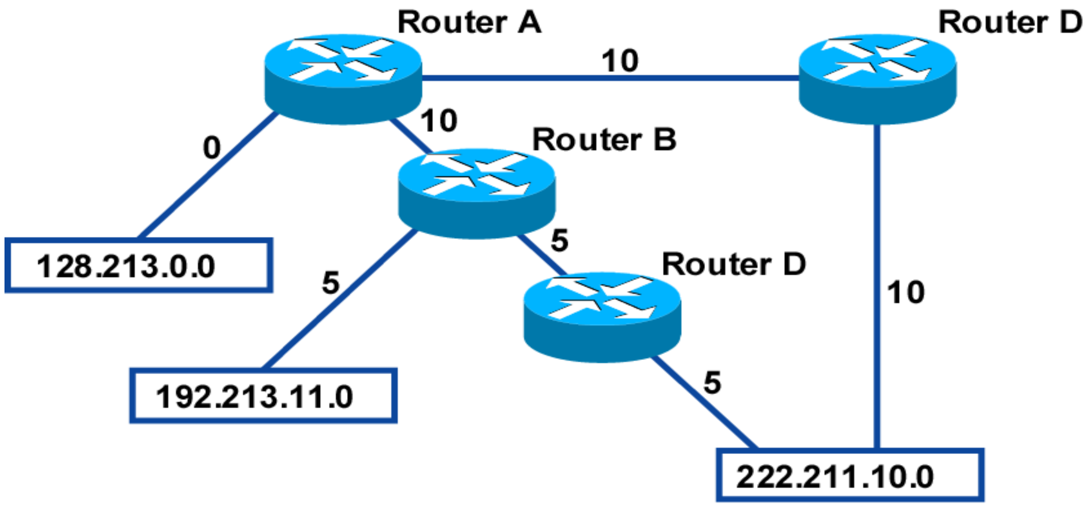
*OSPF propagates link-state advertisements rather than routing table updates.
*LSAs are flooded to all OSPF routers in the area.
*The OSPF link-state database is pieced together from the LSAs generated by the OSPF routers.
*OSPF uses the SPF algorithm to calculate the shortest path to a destination.
-Link = router interface
-State = description of an interface and its relationship to neighboring routers

OSPF Hierarchical Routing



*Consists of areas and autonomous systems
*Minimizes routing update traffic

Shortest Path First Algorithm



*Places each router at the root of a tree and calculates the shortest path to each destination based on the cumulative cost
*Cost = 108/bandwidth (bps)

Configuring Single Area OSPF

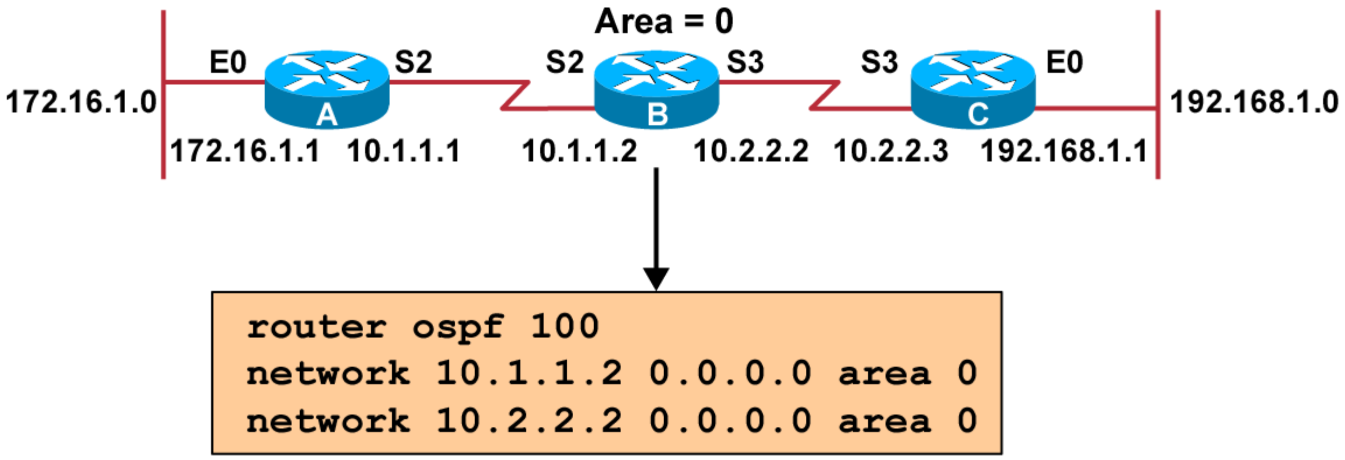
MONA(config)#router ospf *process-id*

**Defines OSPF as the IP routing protocol*

Router(config-router)#network address mask area area-id

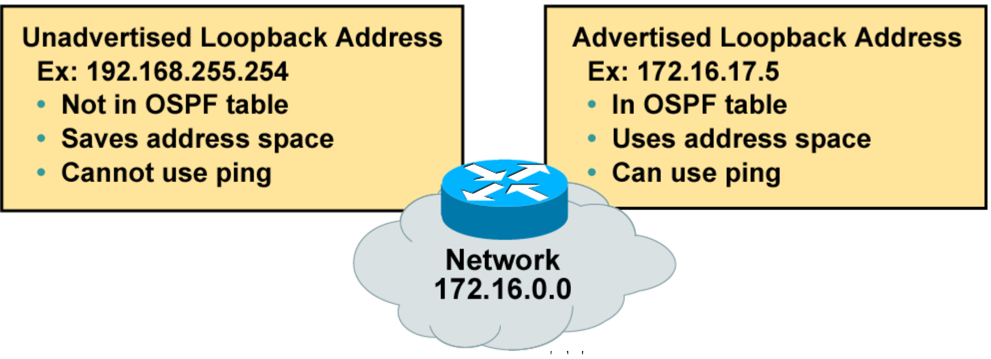
**Assigns networks to a specific OSPF area*

OSPF Configuration Example



```
router ospf 100
network 10.1.1.2 0.0.0.0 area 0
network 10.2.2.2 0.0.0.0 area 0
```

Configuring Loopback Interfaces



Unadvertised Loopback Address
Ex: 192.168.255.254
- Not in OSPF table
- Saves address space
- Cannot use ping

Advertised Loopback Address
Ex: 172.16.17.5
- In OSPF table
- Uses address space
- Can use ping

Route

*Number by which the router is known to OSPF
*Default: The highest IP address on an active interface at the moment of OSPF process startup
*Can be overridden by a loopback interface: Highest IP address of any active loopback interface

Verifying the OSPF Configuration

```
MONA#show ip protocols
```

*Verifies that OSPF is configured

```
MONA#show ip route
```

* Displays all the routes learned by the router

```
MONA#show ip ospf interface
```

* Displays area-ID and adjacency information

```
MONA#show ip ospf neighbor
```

* Displays OSPF-neighbor information on a per-interface basis

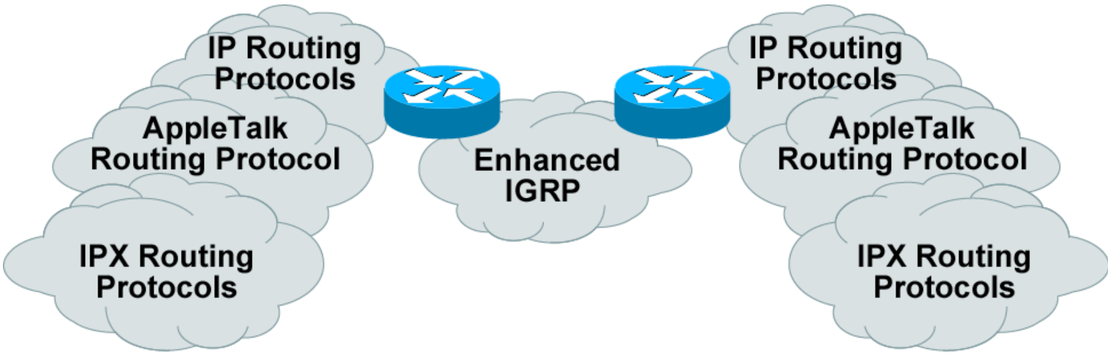
OSPF debug commands

```
MONA#debug ip ospf events
      OSPF:hello with invalid timers on interface Ethernet0
      hello interval received 10 configured 10
      net mask received 255.255.255.0 configured 255.255.255.0
      dead interval received 40 configured 30
MONA# debug ip ospf packet
       OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.117
          aid:0.0.0.0 chk:6AB2 aut:0 auk:
       MONA#debug ip ospf packet
       OSPF: rcv. v:2 t:1 l:48 rid:200.0.0.116
          aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0
```

□

Enabling EIGRP

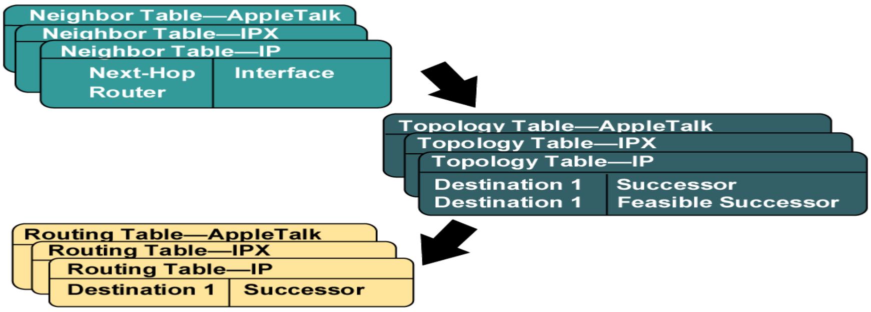
Introducing EIGRP



EIGRP supports:

*Rapid convergence
*Reduced bandwidth usage
*Multiple network-layer protocols

EIGRP Terminology



Comparing EIGRP and IGRP

*Similar metric
*Same load balancing
*Improved convergence time
*Reduced network overhead

Configuring EIGRP

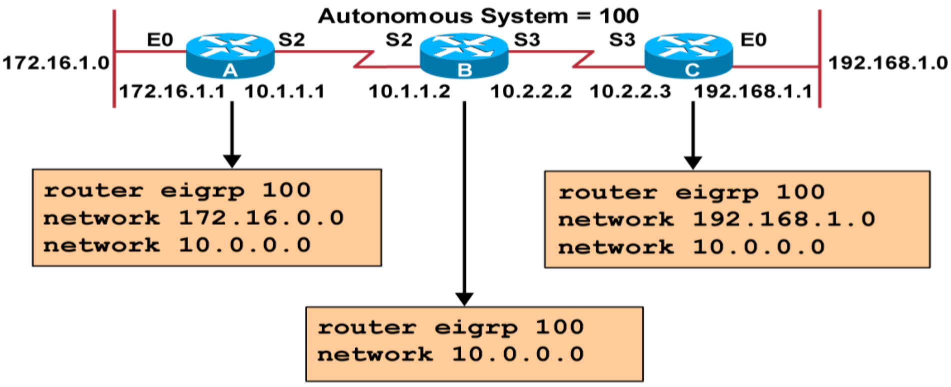
MONA(config)#router eigrp *autonomous-system*

*Defines EIGRP as the IP routing protocol

MONA(config-router)#network *network-number*

*Selects participating attached networks

EIGRP Configuration Example



```
router eigrp 100
network 172.16.0.0
network 10.0.0.0
```

```
router eigrp 100
network 192.168.1.0
network 10.0.0.0
```

```
router eigrp 100
network 10.0.0.0
```

Verifying the EIGRP Configuration

MONA#show ip eigrp neighbors

*Displays the neighbors discovered by IP EIGRP

MONA#show ip eigrp topology

*Displays the IP EIGRP topology table

MONA#show ip route eigrp

*Displays current EIGRP entries in the routing table

MONA#show ip protocols

*Displays the parameters and current state of the active routing protocol process

MONA#show ip eigrp traffic

*Displays the number of IP EIGRP packets sent and received

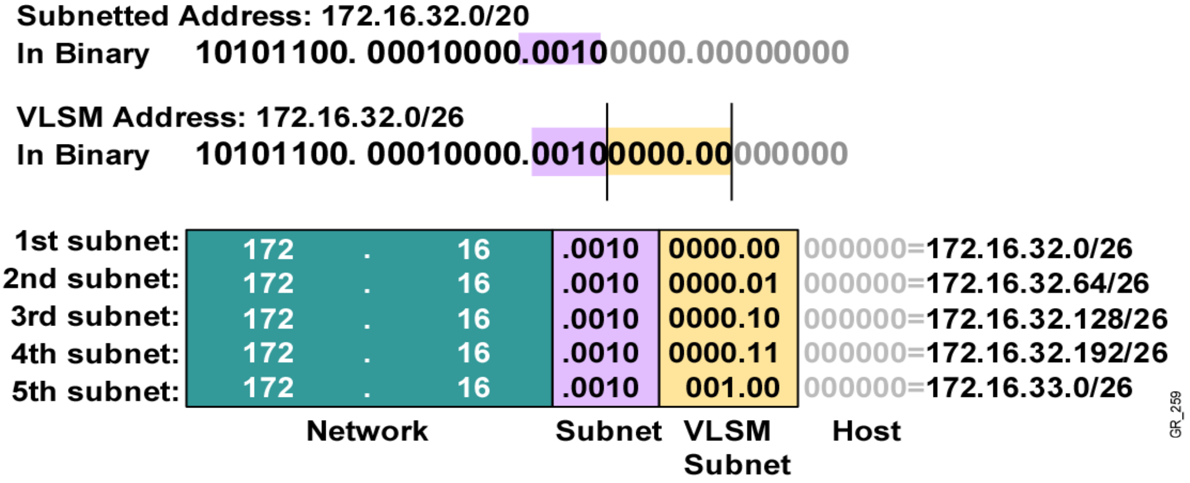
debug ip eigrp Command

MONA#debug ip eigrp

```
IP-EIGRP: Processing incoming UPDATE packet
IP-EIGRP: Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960IP-EIGRP:
Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960IP-EIGRP: Ext
192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960
IP-EIGRP: 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.43.0 255.255.255.0 metric 371200 - 256000 115200
IP-EIGRP: 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.246.0 255.255.255.0 metric 46310656 - 45714176 596480
IP-EIGRP: 172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 172.69.40.0 255.255.255.0 metric 2272256 - 1657856 614400
IP-EIGRP: 192.135.245.0 255.255.255.0, - do advertise out Ethernet0/1
IP-EIGRP: Ext 192.135.245.0 255.255.255.0 metric 40622080 - 40000000 622080
IP-EIGRP: 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1
```

Variable-LengthSubnet Masks

Calculating VLSMs



Subnetted Address: 172.16.32.0/20

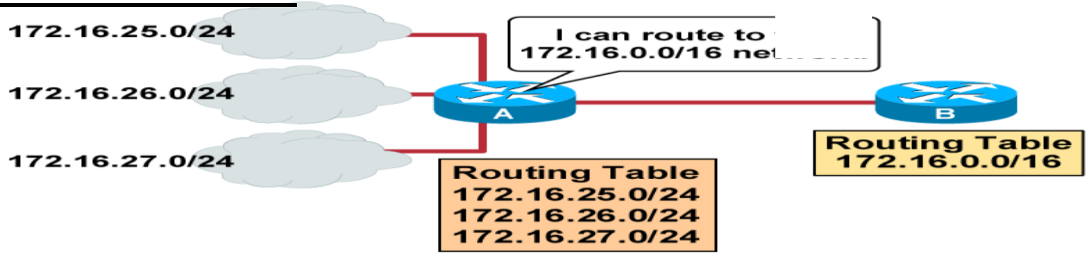
In Binary 10101100. 00010000.00100000.00000000

VLSM Address: 172.16.32.0/26

In Binary 10101100. 00010000.00100000.00000000

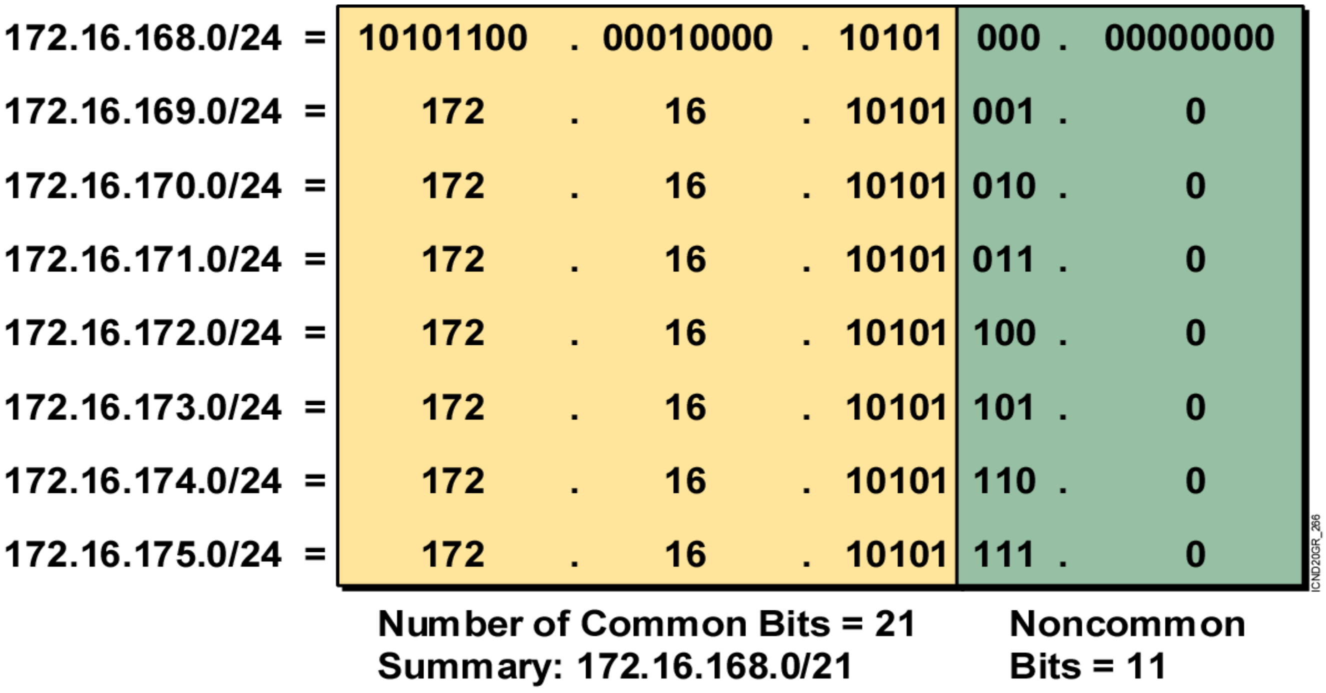
	Network		Subnet	VLSM Subnet	Host
1st subnet:	172 .	16	.0010	0000.00	000000=172.16.32.0/26
2nd subnet:	172 .	16	.0010	0000.01	000000=172.16.32.64/26
3rd subnet:	172 .	16	.0010	0000.10	000000=172.16.32.128/26
4th subnet:	172 .	16	.0010	0000.11	000000=172.16.32.192/26
5th subnet:	172 .	16	.0010	001.00	000000=172.16.33.0/26

What Is Route Summarization?



***Routing protocols can summarize addresses of several networks into one address**

Summarizing Within an Octet



172.16.168.0/24	=	10101100	.	00010000	.	10101	000	.	00000000
172.16.169.0/24	=	172	.	16	.	10101	001	.	0
172.16.170.0/24	=	172	.	16	.	10101	010	.	0
172.16.171.0/24	=	172	.	16	.	10101	011	.	0
172.16.172.0/24	=	172	.	16	.	10101	100	.	0
172.16.173.0/24	=	172	.	16	.	10101	101	.	0
172.16.174.0/24	=	172	.	16	.	10101	110	.	0
172.16.175.0/24	=	172	.	16	.	10101	111	.	0

ICND20GR_266

Number of Common Bits = 21
Summary: 172.16.168.0/21

Noncommon
Bits = 11

Implementation Considerations

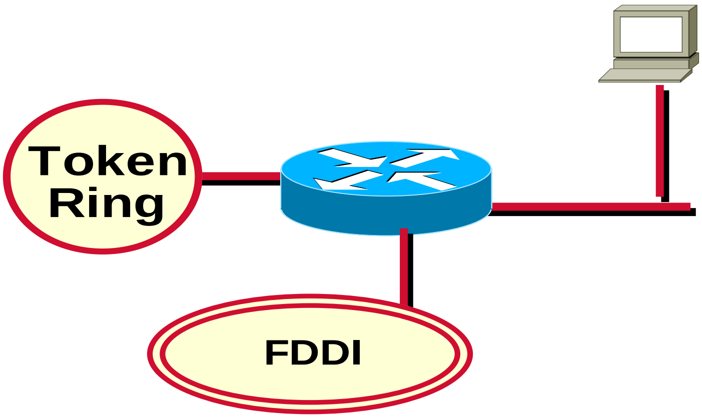
*Multiple IP addresses must have the same highest-order bits.
*Routing decisions are made based on the entire address.
Routing protocols must carry the prefix (subnet mask) length.

Route Summarization Operation in Cisco Routers

192.16.5.33	/32	Host
192.16.5.32	/27	Subnet
192.16.5.0	/24	Network
192.16.0.0	/16	Block of Networks
0.0.0.0	/0	Default

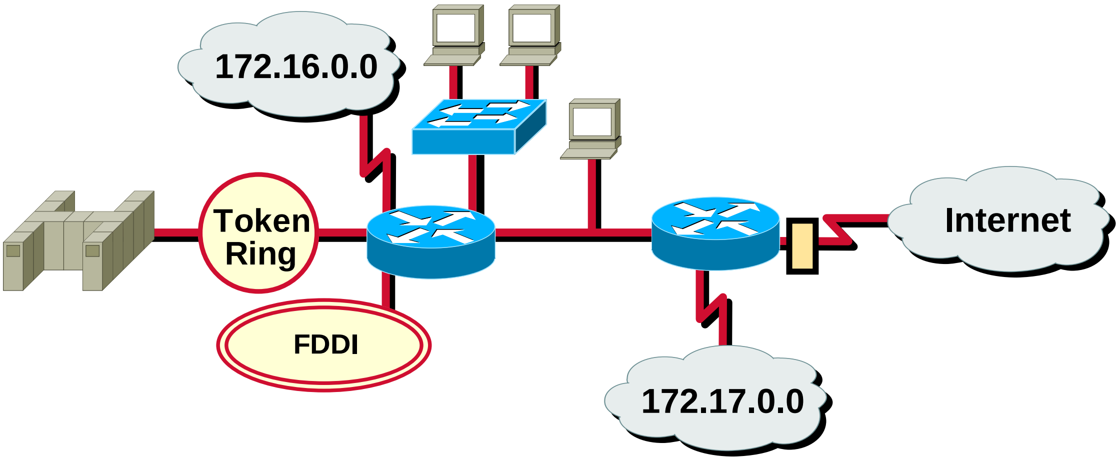
*Supports host-specific routes, blocks of networks, default routes
*Routers use the longest match

Why Use Access Lists?



*Manage IP Traffic as network access grows

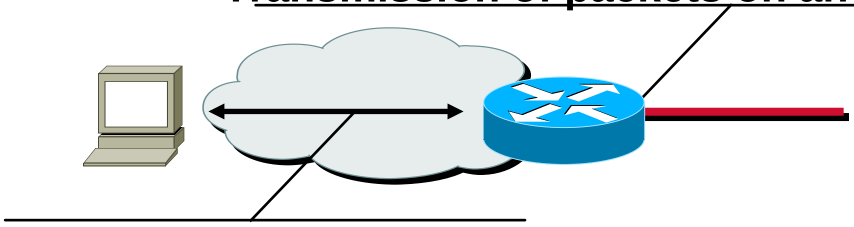
Why Use Access Lists?



*Manage IP traffic as network access grows
*Filter packets as they pass through the router

Access List Applications

Transmission of packets on an interface

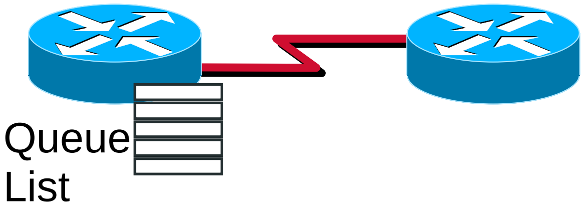


Virtual terminal line access (IP)

*Permit or deny packets moving through the router
*Permit or deny vty access to or from the router
*Without access lists all packets could be transmitted onto all parts of your network

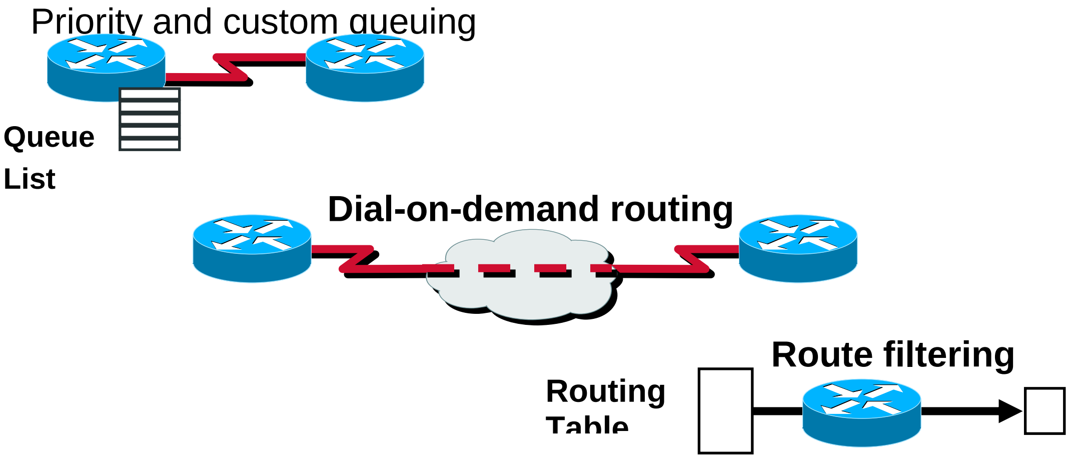
Other Access List Uses

Priority and custom queuing



Special handling for traffic based on packet tests

Other Access List Uses



Priority and custom queuing

Queue List

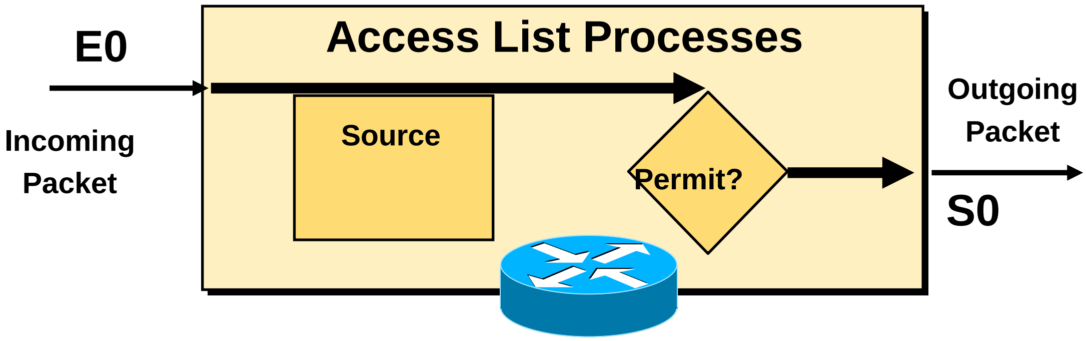
Dial-on-demand routing

Route filtering

Routing Table

Special handling for traffic based on packet tests

What Are Access Lists?



E0

Incoming Packet

Access List Processes

Source

Permit?

Outgoing Packet

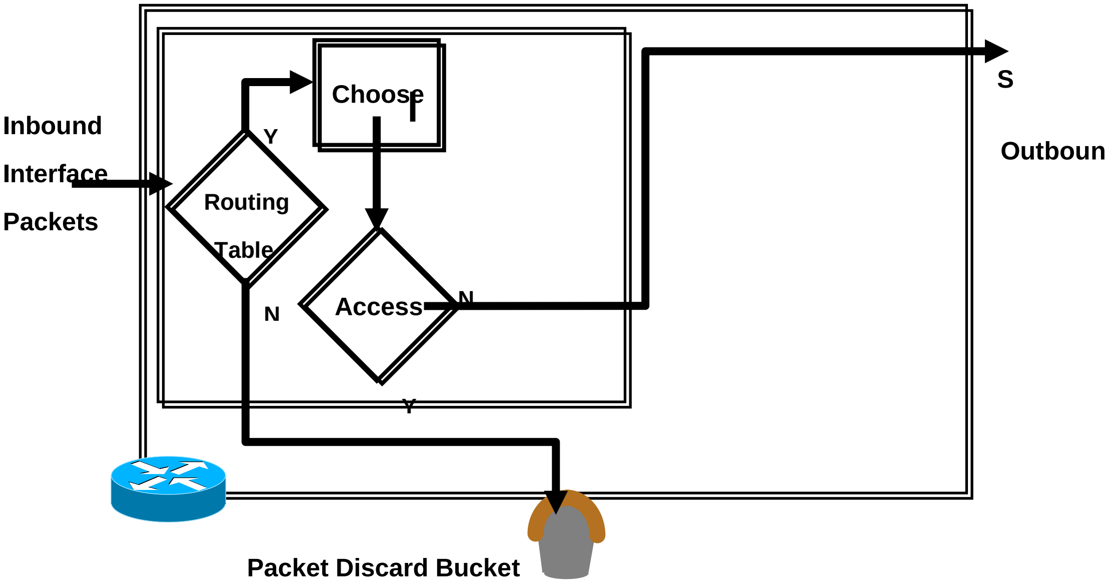
S0

*Standard
-Checks Source address
-Generally permits or denies entire protocol suite

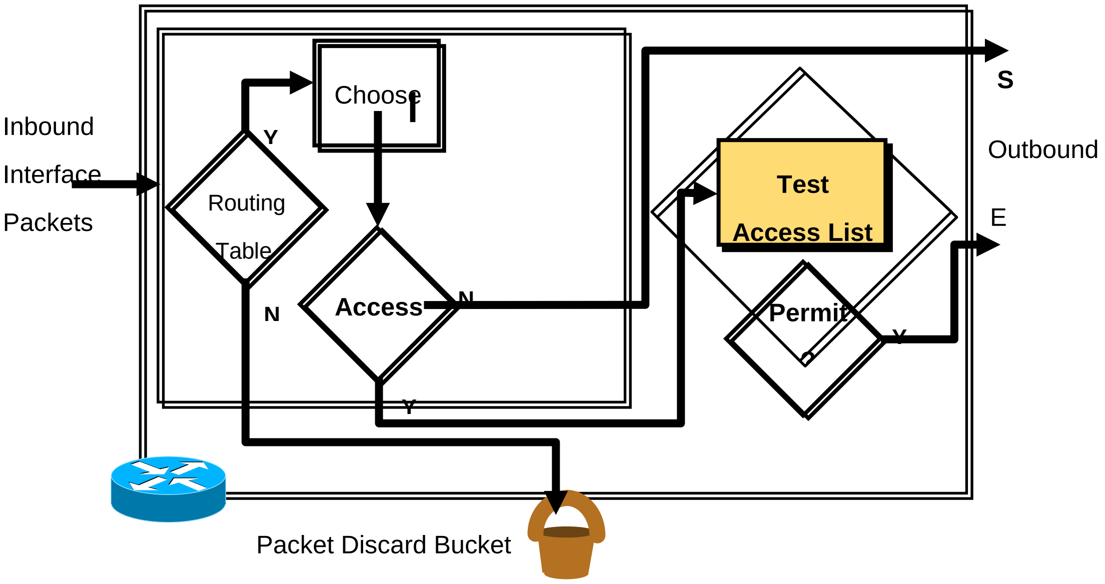
What Are Access Lists?

*Standard
-Checks Source address
-Generally permits or denies entire protocol suite
*Extended
-Checks Source and Destination address
-Generally permits or denies specific protocols
*Inbound or Outbound

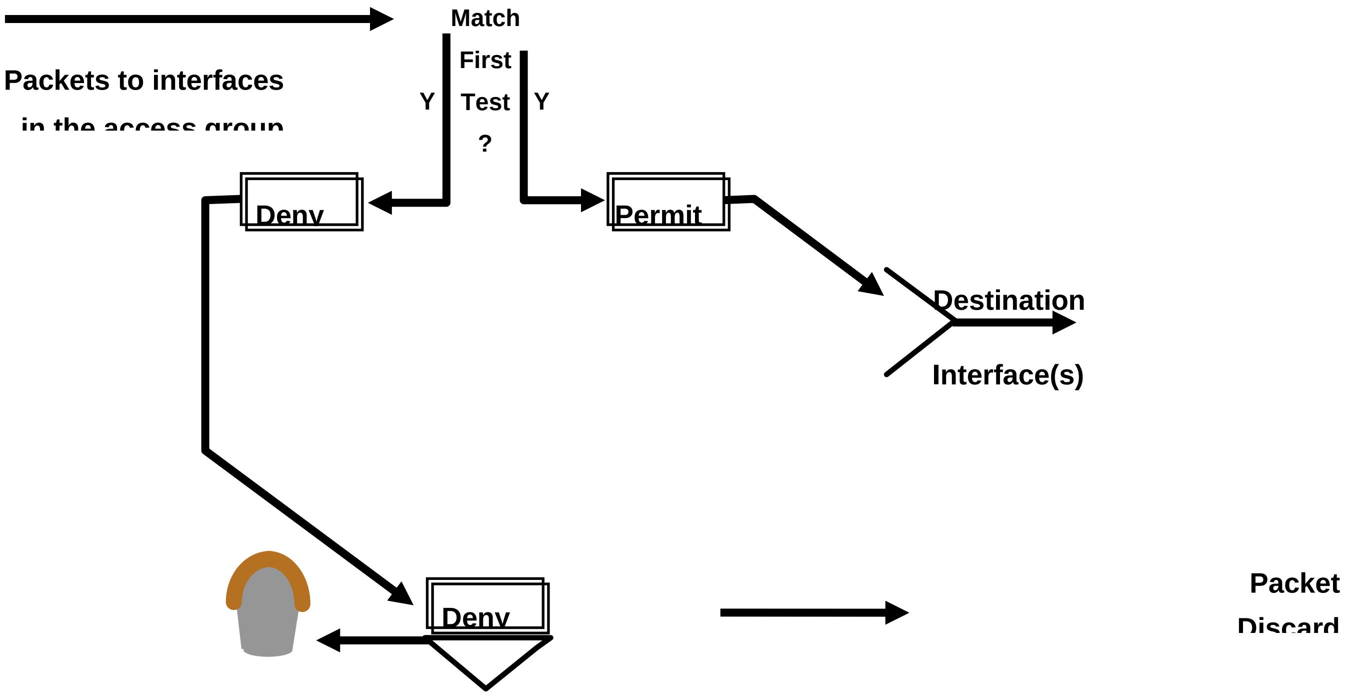
Outbound Access Lists



Outbound Access Lists



A List of Tests: Deny or Permit



Packets to interfaces

in the access group

Match

First

Test

?

Y

Y

Deny

Permit

Destination

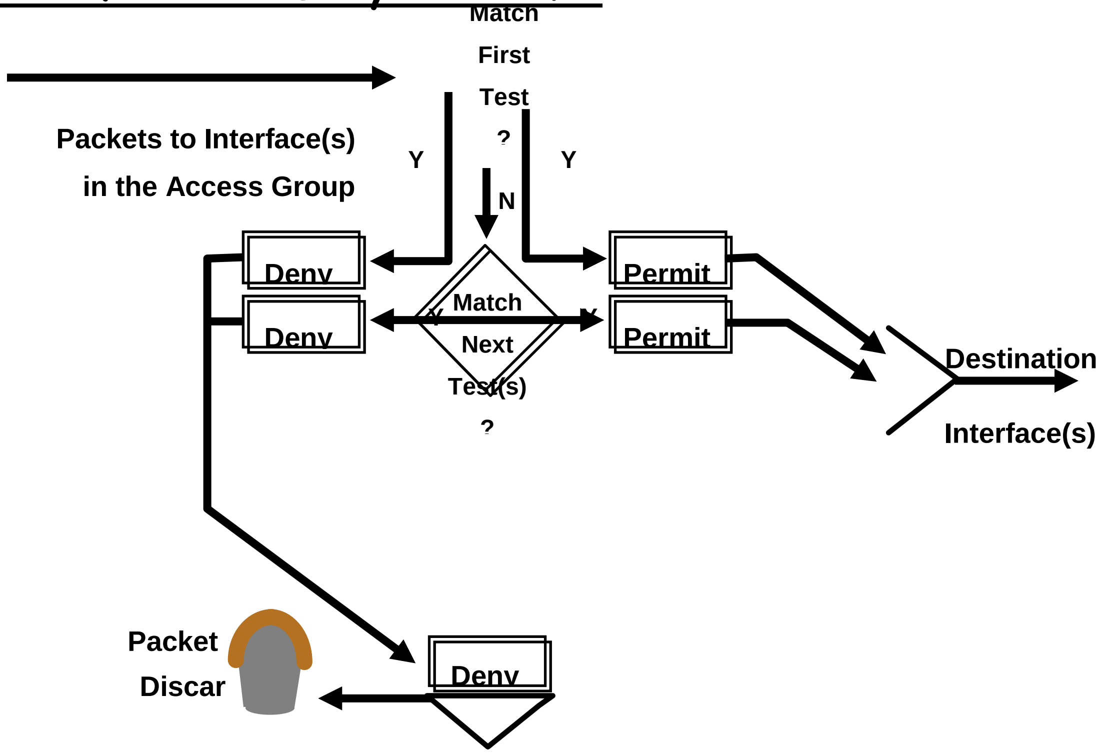
Interface(s)

Deny

Packet

Discard

A List of Tests: Deny or Permit



Packets to Interface(s)

in the Access Group

Match

First

Test

?

Y

Y

N

Deny

Deny

Match

Next

Test(s)

?

Y

Y

Permit

Permit

Destination

Interface(s)

Packet

Discar

Deny

Access List Configuration Guidelines

*Access list numbers indicate which protocol is filtered

*One access list per interface, per protocol, per direction

*The order of access list statements controls testing

*Most restrictive statements should be at the top of list

*There is an implicit deny any as the last access list test—every list should have at least one permit statement

*Create access lists before applying them to interfaces

*Access list, filter traffic going through the router; they do not apply to traffic originated from the router

Access List Command Overview

Step 1: Set parameters for this access list test
statement (which can be one of several statements)

MONA(config)#   access-list *access-list-number* { permit | deny } {test conditions }

Access List Command Overview

Step 1: Set parameters for this access list test
statement (which can be one of several statements)

MONA(config)#

access-list *access-list-number* { permit | deny } { test conditions }

Step 2: Enable an interface to use the specified
access list

MONA(config-if)#

{ *protocol* } access-group *access-list-number {in | out}*

IP Access lists are numbered 1-99 or 100-199

How to Identify Access Lists

Access List Type	Number Range/Identifier
IP Standard	1-99

*Standard IP lists (1 to 99) test conditions of all IP packets from source addresses

How to Identify Access Lists

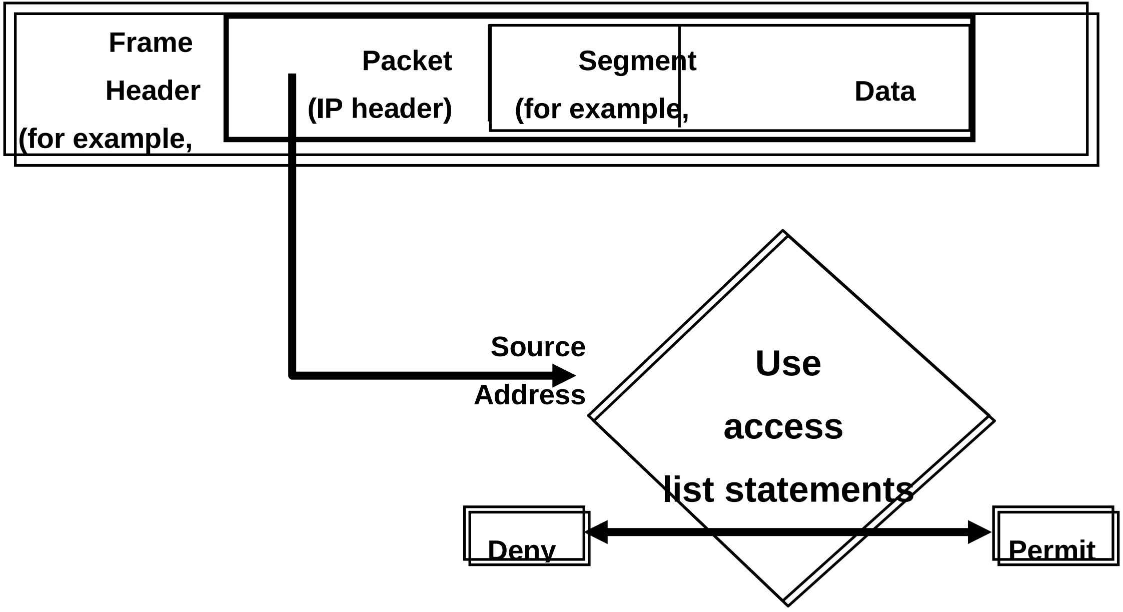
Access List Type	Number Range/Identifier
IP Standard Extended Named	1-99 100-199 Name (Cisco IOS 11.2 and later)
IPX Standard Extended SAP filters Named	800-899 900-999 1000-1099 Name (Cisco IOS 11.2. F and later)

*Standard IP lists (1 to 99) test conditions of all IP packets from source addresses

*Extended IP lists (100 to 199) can test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports

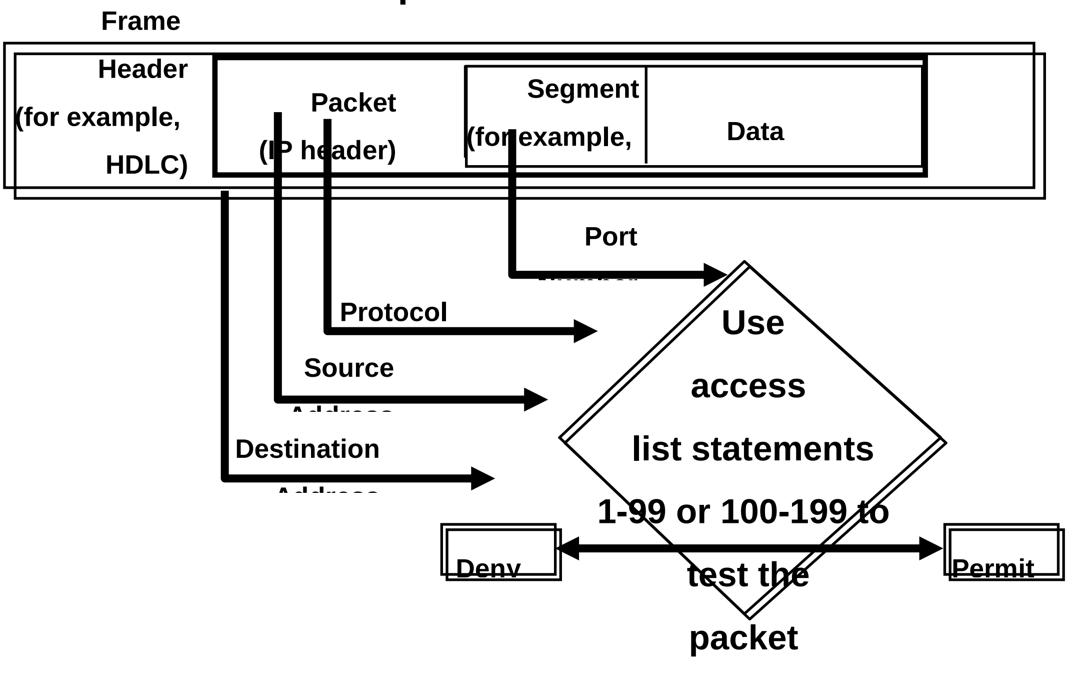
*Other access list number ranges test conditions for other networking protocols

Testing Packets with Standard Access Lists

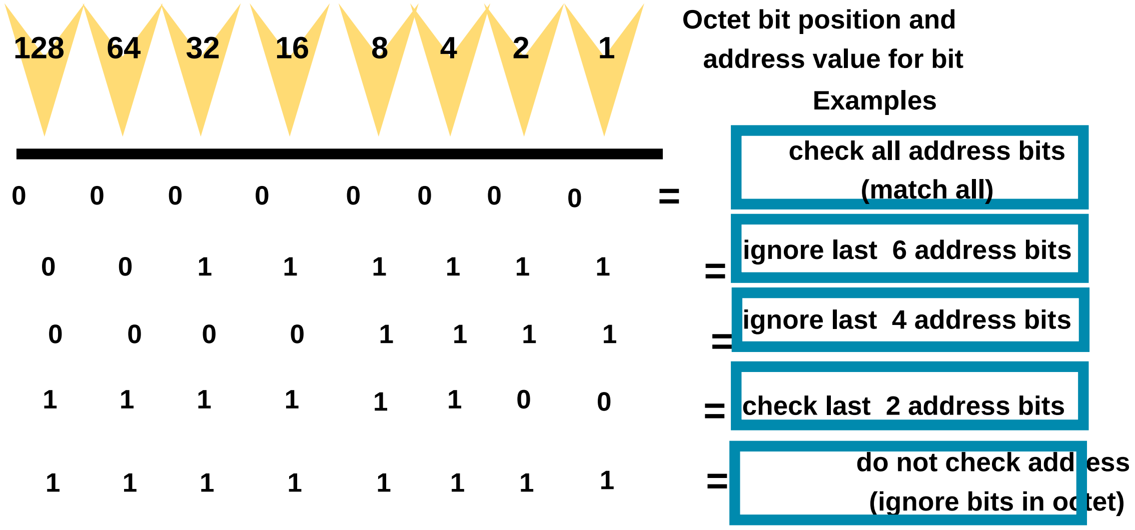


Testing Packets with Extended Access Lists

An Example from a TCP/IP Packet



Wildcard Bits: How to Check the Corresponding Address Bits



Octet bit position and address value for bit

Examples

128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	=	check all address bits (match all)
0	0	1	1	1	1	1	1	=	ignore last 6 address bits
0	0	0	0	1	1	1	1	=	ignore last 4 address bits
1	1	1	1	1	1	0	0	=	check last 2 address bits
1	1	1	1	1	1	1	1	=	do not check address (ignore bits in octet)

*0 means check corresponding address bit value
*1 means ignore value of corresponding address bit

Standard IP Access List Configuration

MONA(config)#

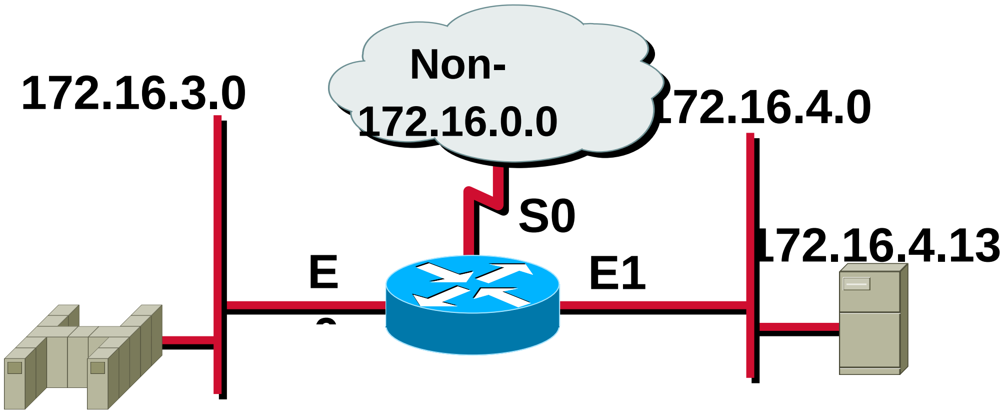
access-list *access-list-number* {permit|deny} *source* [*mask*]

*Sets parameters for this list entry
*IP standard access lists use 1 to 99
*Default wildcard mask = 0.0.0.0
*“no access-list *access-list-number*” removes entire access-list

Standard IP Access List Configuration

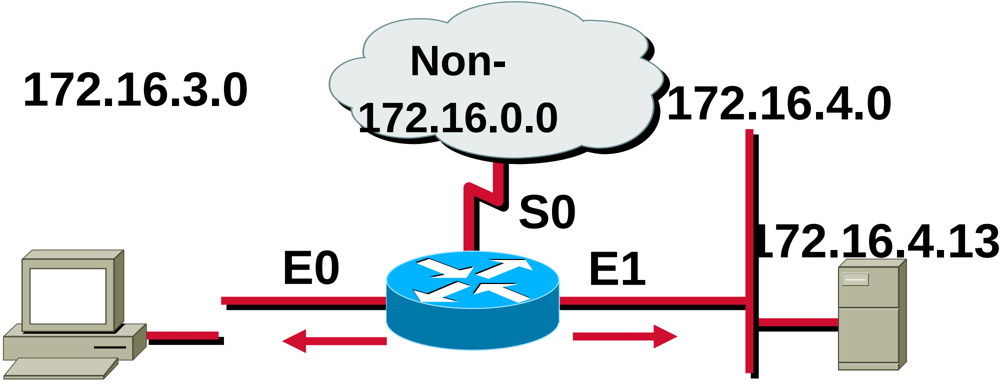
MONA(config)#
access-list *access-list-number* {permit|deny} *source* [*mask*]
*Sets parameters for this list entry
*IP standard access lists use 1 to 99
*Default wildcard mask = 0.0.0.0
*“no access-list *access-list-number*” removes entire access-list
MONA(config-if)#
ip access-group *access-list-number* { in | out }
*Activates the list on an interface
*Sets inbound or outbound testing
*Default = Outbound
*“no ip access-group *access-list-number*” removes access-list from the interface

Standard IP Access List Example 1



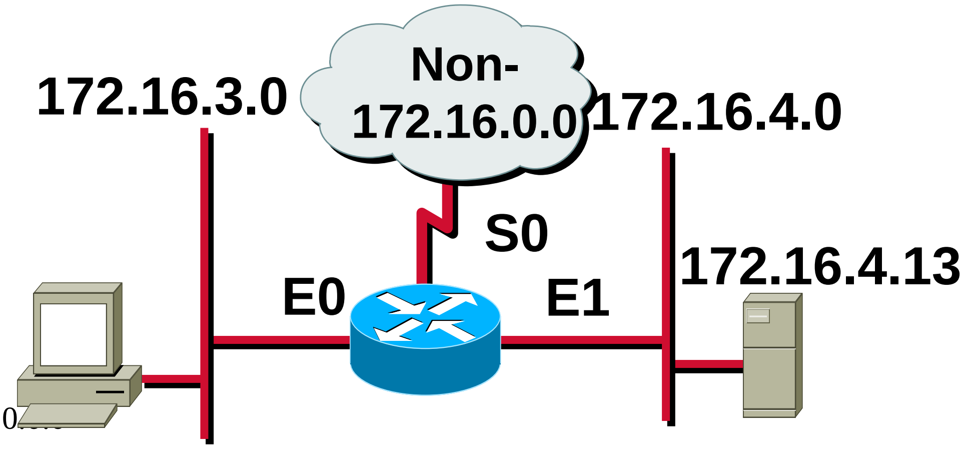
access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

Standard IP Access List Example 1



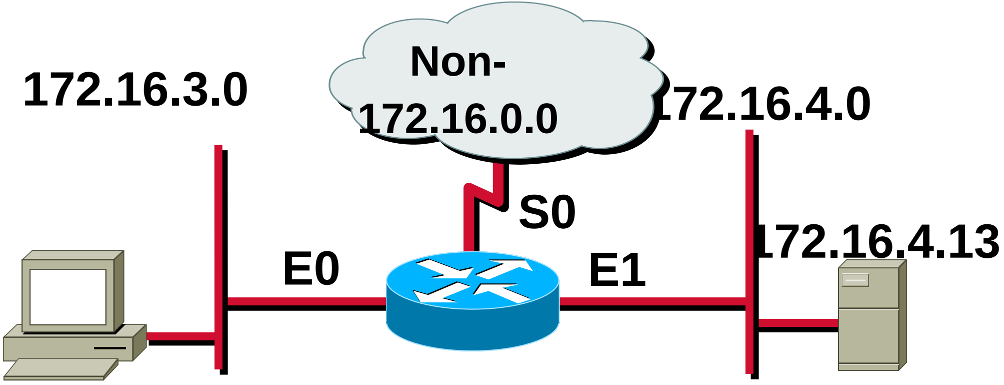
access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
Permit my network only

Standard IP Access List Example 2



access-list 1 deny 172.16.4.13 0.0.0.0
Deny a specific host

Standard IP Access List Example 2

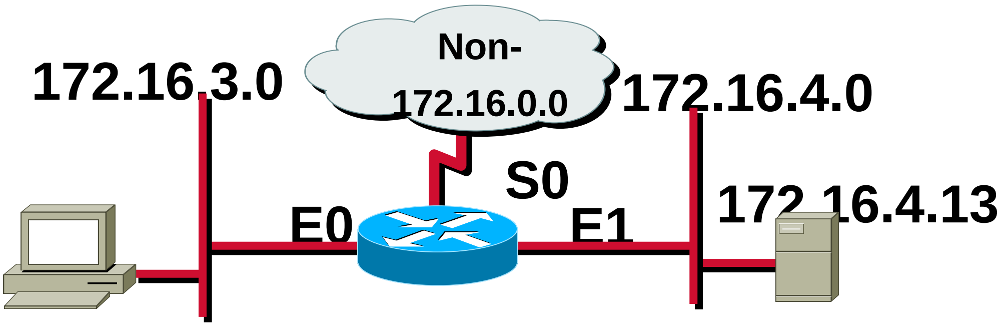


access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
Deny a specific host

Standard IP Access List Example 2

access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
interface ethernet 0
ip access-group 1 out

Standard IP Access List Example 3



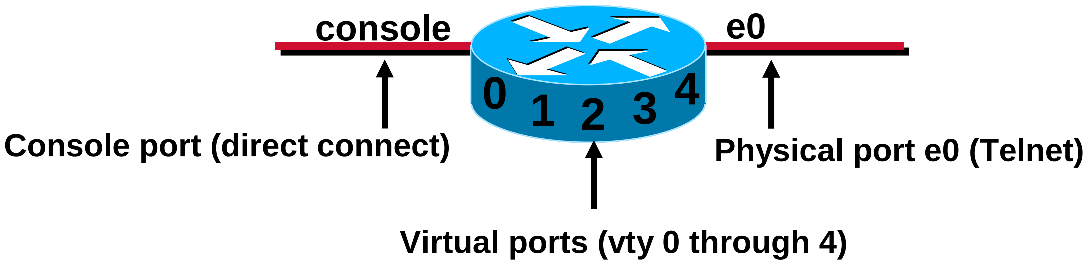
access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
Deny a specific subnet

Standard IP Access ListExample 3

access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)
interface ethernet 0
ip access-group 1 out

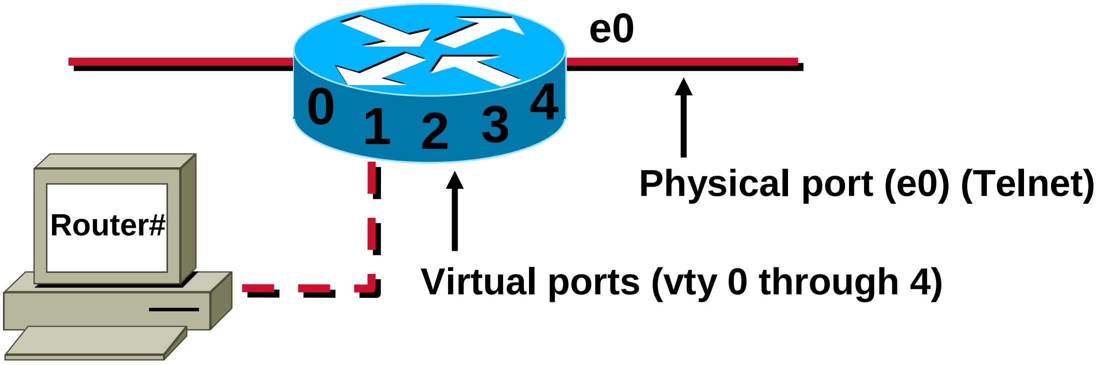
Control vty Access With Access Class

Filter Virtual Terminal (vty) Access to a Router


console
e0
0
1
2
3
4
Console port (direct connect)
Physical port e0 (Telnet)
Virtual ports (vty 0 through 4)

*Five virtual terminal lines (0 through 4)
*Filter addresses that can access into the router’s vty ports
*Filter vty access out from the router

How to Control vty Access



*Setup IP address filter with standard access list statement
*Use line configuration mode to filter access with the *access-class* command
*Set identical restrictions on all vtys

Virtual Terminal Line Commands

MONA(config)#
line vty#*{vty#* | *vty-range*}

*Enters configuration mode for a vty or vty range

MONA(config-line)#
access-class *access-list-number* {in|out}

*Restricts incoming or outgoing vty connections for address in the access list

<u>Virtual Terminal Access Example</u>

Controlling Inbound Access

```
access-list 12 permit 192.89.55.0 0.0.0.255
!
line vty 0 4
 access-class 12 in
```

Permits only hosts in network 192.89.55.0 to connect to the router’s vtys

Configuring Extended IP Access Lists

Standard versus External Access List

Standard	nded
Filters Based on Source.	Filters Based on Source and estination.
Permit or deny entire TCP/IP protocol suite.	Specifies a specific IP protocol and port number.
Range is 1 through 99	Range is 100 through 199.

Extended IP Access List Configuration

MONA(config)#

access-list *access-list-number* { permit | deny } *protocol source source-wildcard [operator port] destination destination-wildcard* [*operator port*] [established] [log]

*Sets parameters for this list entry

Extended IP Access List Configuration

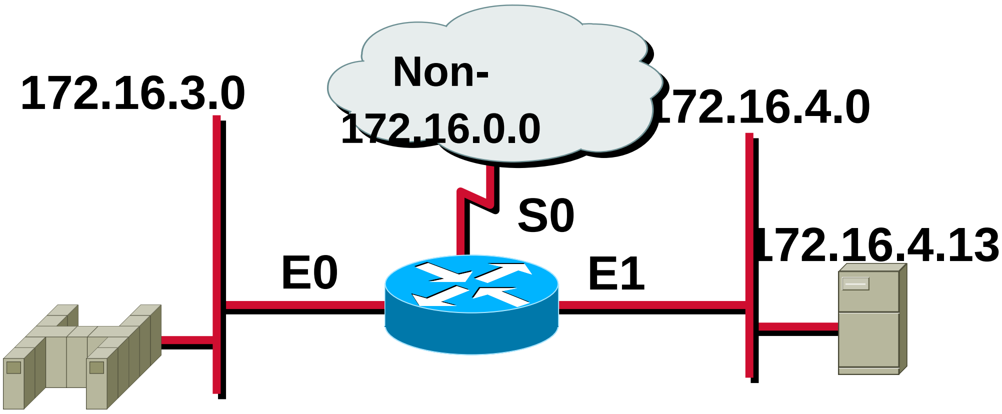
MONA(config)# access-list *access-list-number*
{ permit | deny } *protocol source source-wildcard [operator port] destination destination-wildcard* [*operator port*] [established] [log]

*Sets parameters for this list entry

MONA(config-if)# ip access-group *access-list-number* { in | out }

*Activates the extended list on an interface

Extended Access List Example 1



```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
```

*Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0

*Permit all other traffic

Extended Access List Example 1

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
```

*Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0

Permit all other traffic

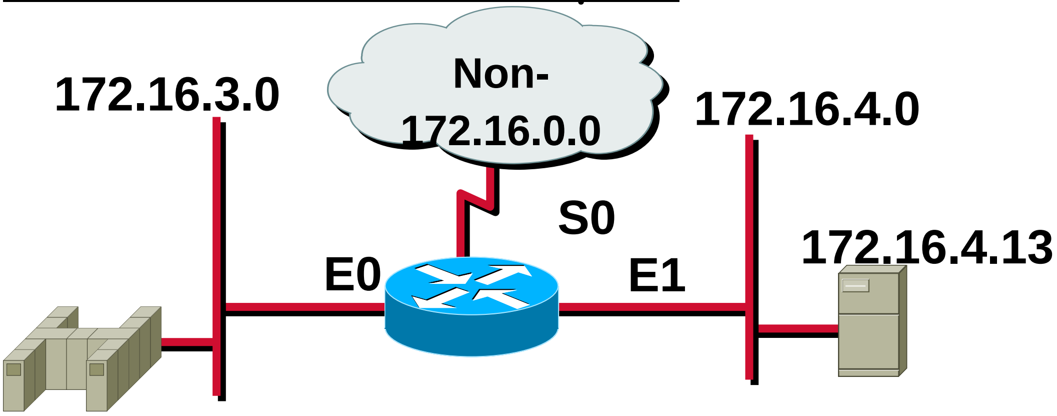
Extended Access List Example 1

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
interface ethernet 0
ip access-group 101 out
```

Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0

Permit all other traffic

Extended Access List Example 2



```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
```

*Deny only Telnet from subnet 172.16.4.0 out of E0

*Permit all other traffic

Extended Access List Example 2

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
access-list 101 permit ip any any
(implicit deny all)
```

*Deny only Telnet from subnet 172.16.4.0 out of E0

*Permit all other traffic

Extended Access List Example 2

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
access-list 101 permit ip any any
(implicit deny all)
interface ethernet 0
ip access-group 101 out
```

*Deny only Telnet from subnet 172.16.4.0 out of E0

Permit all other traffic

Using Named IP Access Lists

*Feature for Cisco IOS Release 11.2 or later

```
MONA(config)#
ip access-list { standard | extended } name
```

*Alphanumeric name string must be unique

Using Named IP Access Lists

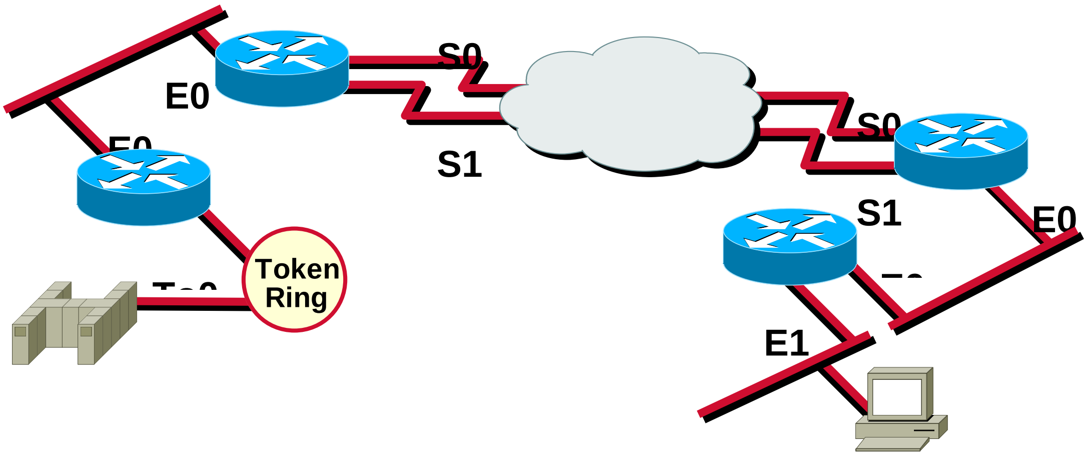
*Feature for Cisco IOS Release 11.2 or later
Router(config)#
ip access-list { standard | extended } name
*Alphanumeric name string must be unique
Router(config {std- | ext-}nacl)#
{ permit | deny } { ip access list test conditions }
{ permit | deny } { ip access list test conditions }
no { permit | deny } { ip access list test conditions }
*Permit or deny statements have no prepended number
*"no" removes the specific test from the named access list

Using Named IP Access Lists

***Feature for Cisco IOS Release 11.2 or later**

MONA(config)# ip access-list { standard | extended } name
*Alphanumeric name string must be unique
Router(config {std- | ext-}nacl)# { permit | deny }
{ ip access list test conditions }
{ permit | deny } { ip access list test conditions }
no { permit | deny } { ip access list test conditions }
*Permit or deny statements have no prepended number
*"no" removes the specific test from the named access list
MONA(config-if)# ip access-group name { in | out }
*Activates the IP named access list on an interface
Access List Configuration Principles
*Order of access list statements is crucial
Recommended: use a text editor on a TFTP server or use PC to cut and paste
*Top-down processing
Place more specific test statements first
*No reordering or removal of statements
Use no access-list number command to remove entire access list
Exception: Named access lists permit removal of individual statements
*Implicit deny all
Unless access list ends with explicit permit any

Where to Place IP Access Lists



*Place extended access lists close to the source
*Place standard access lists close to the destination

Verifying Access Lists

```
MONA#show ip int e0
        Ethernet0 is up, line protocol is up
          Internet address is 10.1.1.11/24
          Broadcast address is 255.255.255.255
          Address determined by setup command
          MTU is 1500 bytes
          Helper address is not set
          Directed broadcast forwarding is disabled
          Outgoing access list is not set
          Inbound  access list is 1
          Proxy ARP is enabled
          Security level is default
          Split horizon is enabled
          ICMP redirects are always sent
          ICMP unreachables are always sent
          ICMP mask replies are never sent
          IP fast switching is enabled
          IP fast switching on the same interface is disabled
          IP Feature Fast switching turbo vector
          IP multicast fast switching is enabled
          IP multicast distributed fast switching is disabled
          <text ommitted>
```

Monitoring Access List Statements

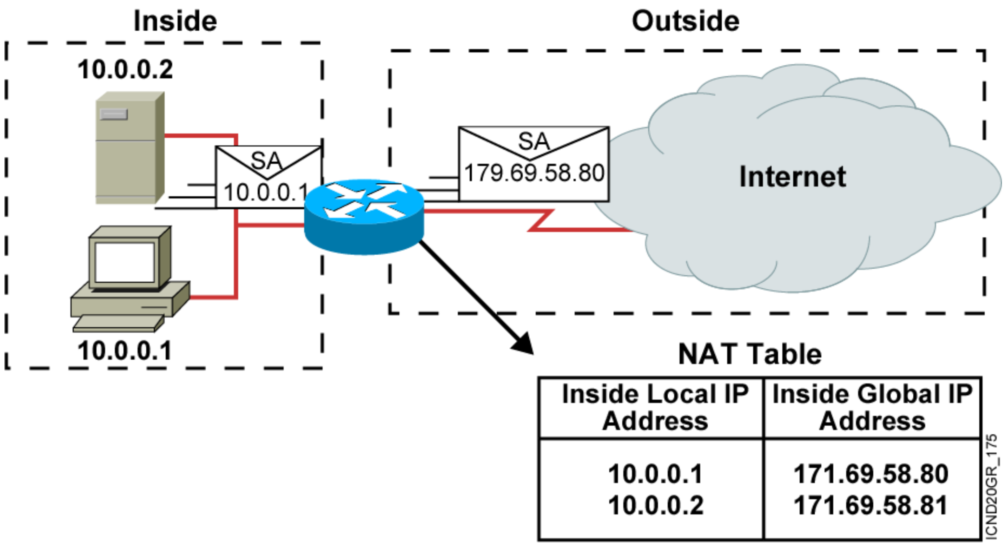
MONA#show {protocol} access-list {*access-list number*}
MONA#show access-lists {*access-list number*}

```
MONA#show access-lists
        Standard IP access list 1
           permit 10.2.2.1
           permit 10.3.3.1
           permit 10.4.4.1
           permit 10.5.5.1
        Extended IP access list 101
           permit tcp host 10.22.22.1 any eq telnet
           permit tcp host 10.33.33.1 any eq ftp
           permit tcp host 10.44.44.1 any eq ftp-data
```

NAT and PAT

Scaling the Network with NAT and PAT

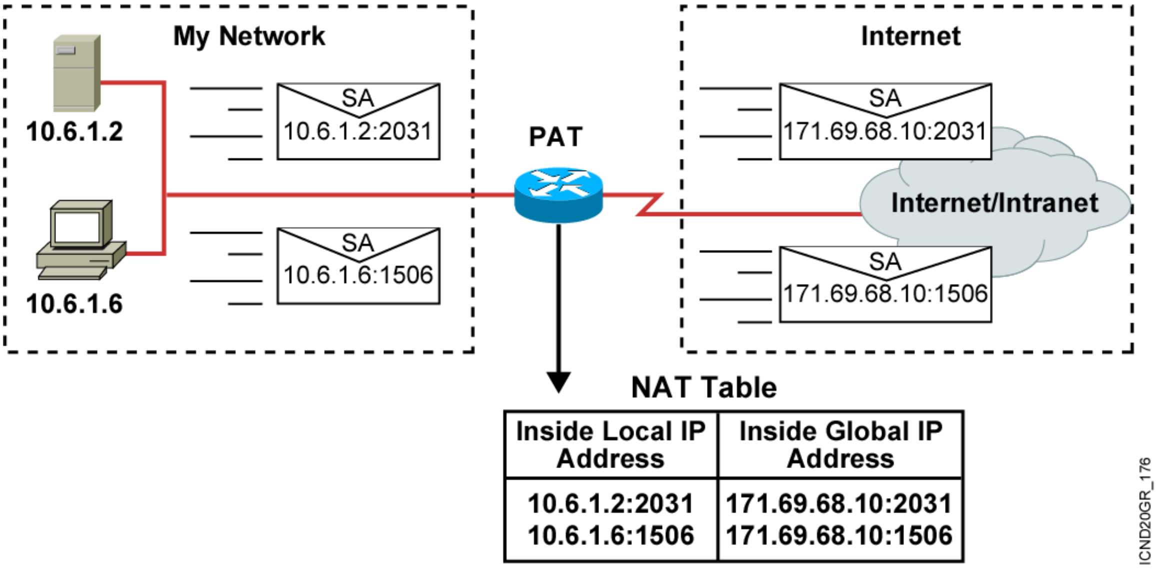
Network Address Translation



Inside Local IP Address	Inside Global IP Address
10.0.0.1	171.69.58.80
10.0.0.2	171.69.58.81

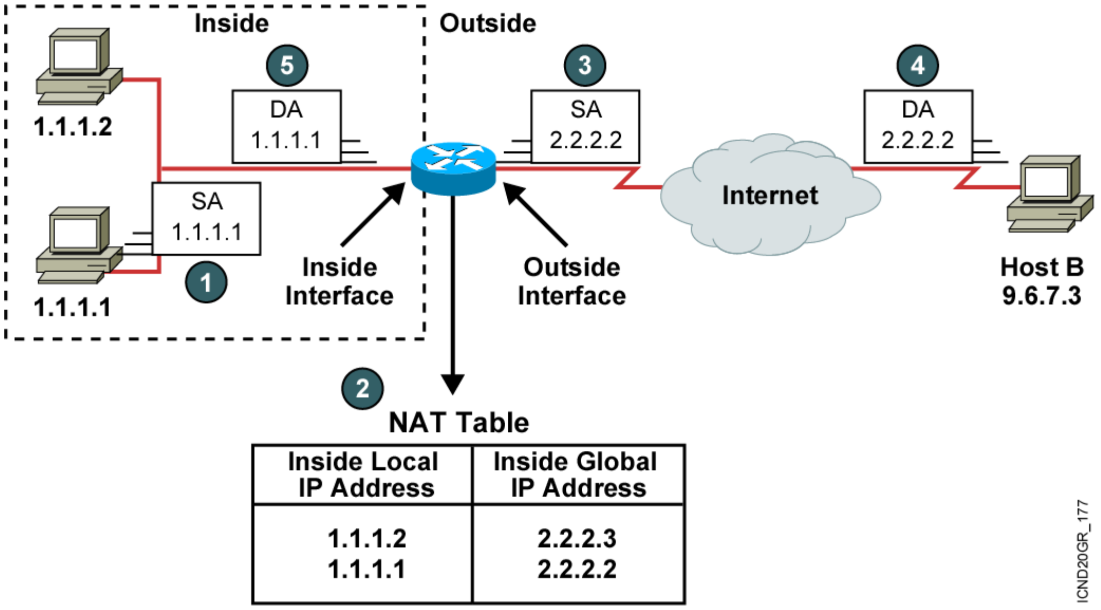
*An IP address is either local or global.
*Local IP addresses are seen in the inside network.

Port Address Translation



Inside Local IP Address	Inside Global IP Address
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506

Translating Inside Source Addresses



Inside Local IP Address	Inside Global IP Address
1.1.1.2	2.2.2.3
1.1.1.1	2.2.2.2

Configuring Static Translation

MONA(config)#ip nat inside source static *local-ip global-ip*

*Establishes static translation between an inside local address and an inside global address

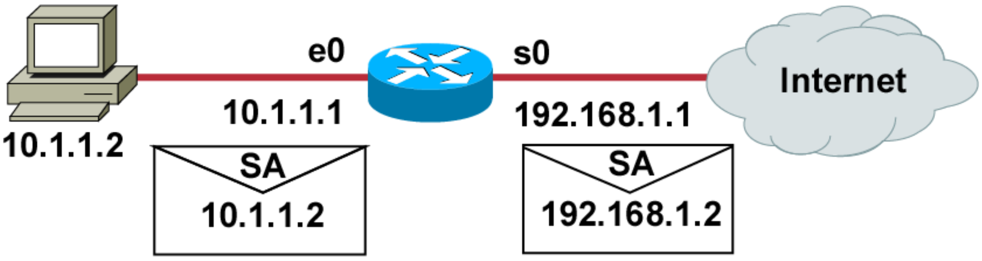
MONA(config-if)#ip nat inside

*Marks the interface as connected to the inside

MONA(config-if)#ip nat outside

*Marks the interface as connected to the outside

Enabling Static NAT Address Mapping Example



```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

ICND20GR_282

Configuring Dynamic Translation

Router(config)#ip nat pool *name start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}

*Defines a pool of global addresses to be allocated as needed

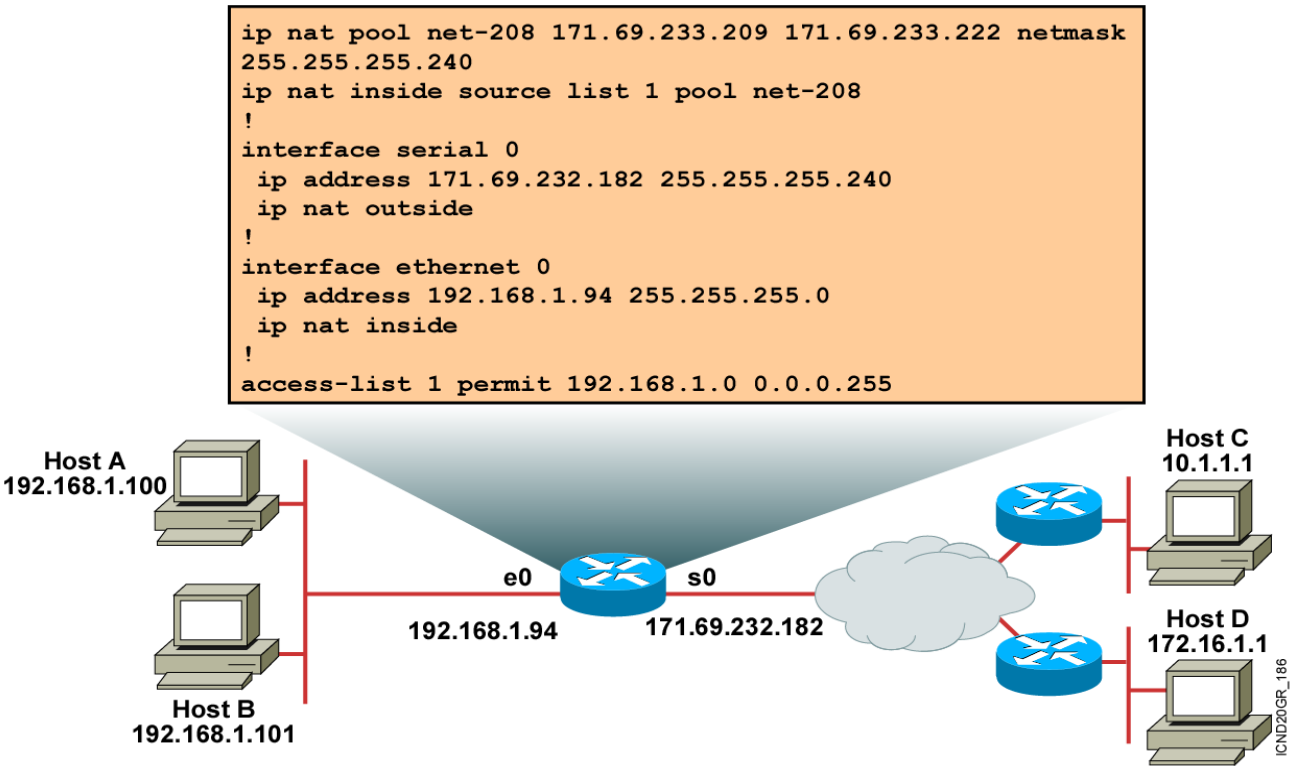
MONA(config)#access-list *access-list-number* permit *source* [*source-wildcard*]

*Defines a standard IP access list permitting those inside local addresses that are to be translated

MONA(config)#ip nat inside source list *access-list-number* pool *name*

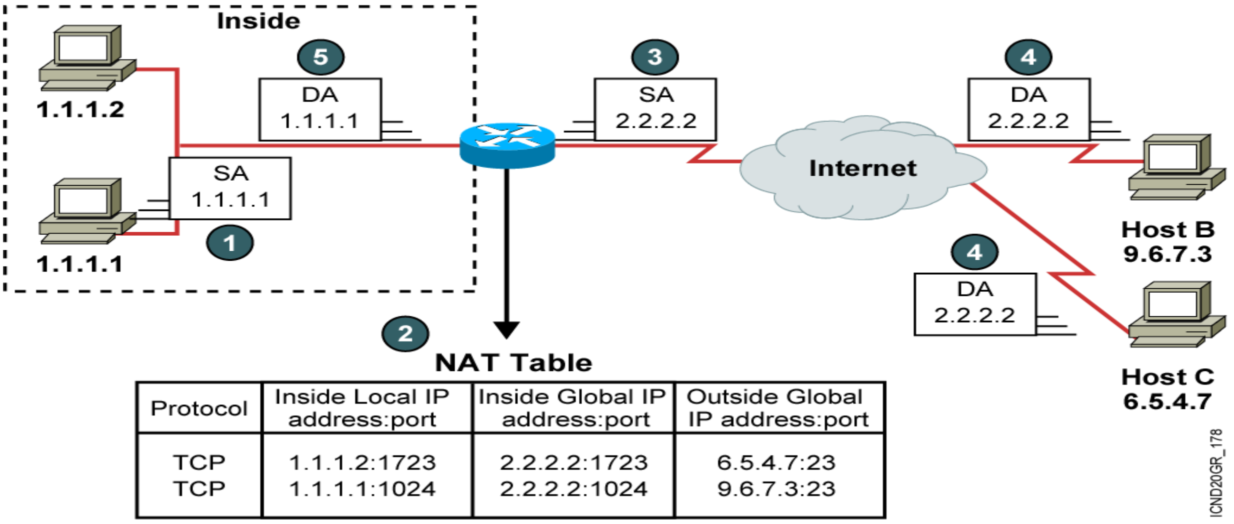
*Establishes dynamic source translation, specifying the access list defined in the prior step

Dynamic Address Translation Example



```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

Overloading an Inside Global Address

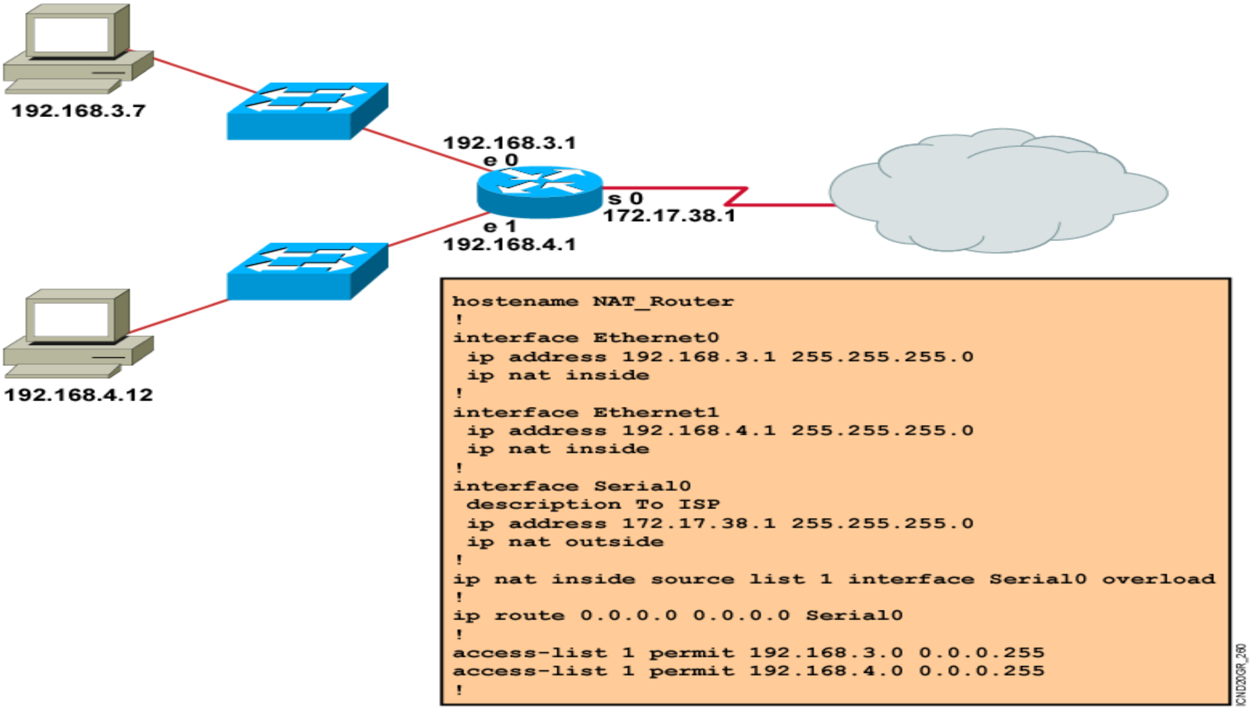


Protocol	Inside Local IP address:port	Inside Global IP address:port	Outside Global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

permit

*Defines a standard IP access list permitting those inside local addresses that are to be translated
MONA(config)#ip nat inside source list
access-list-number interface interface overload
*Establishes dynamic source translation, specifying the access list defined in the prior step

Overloading an Inside Global Address Example



```
hostename NAT_Router
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```

Clearing the NAT Translation Table

Router#clear ip nat translation *

*Clears all dynamic address translation entries
MONA#clear ip nat translation inside *global-ip*
local-ip [outside *local-ip global-ip*]
*Clears a simple dynamic translation entry containing an inside translation, or both inside and outside translation
MONA#clear ip nat translation outside
local-ip global-ip
*Clears a simple dynamic translation entry containing an outside translation
MONA#clear ip nat translation protocol inside *global-ip*
global-port local-ip local-port [outside *local-ip*
local-port global-ip global-port]
*Clears an extended dynamic translation entry

Displaying Information with show Commands

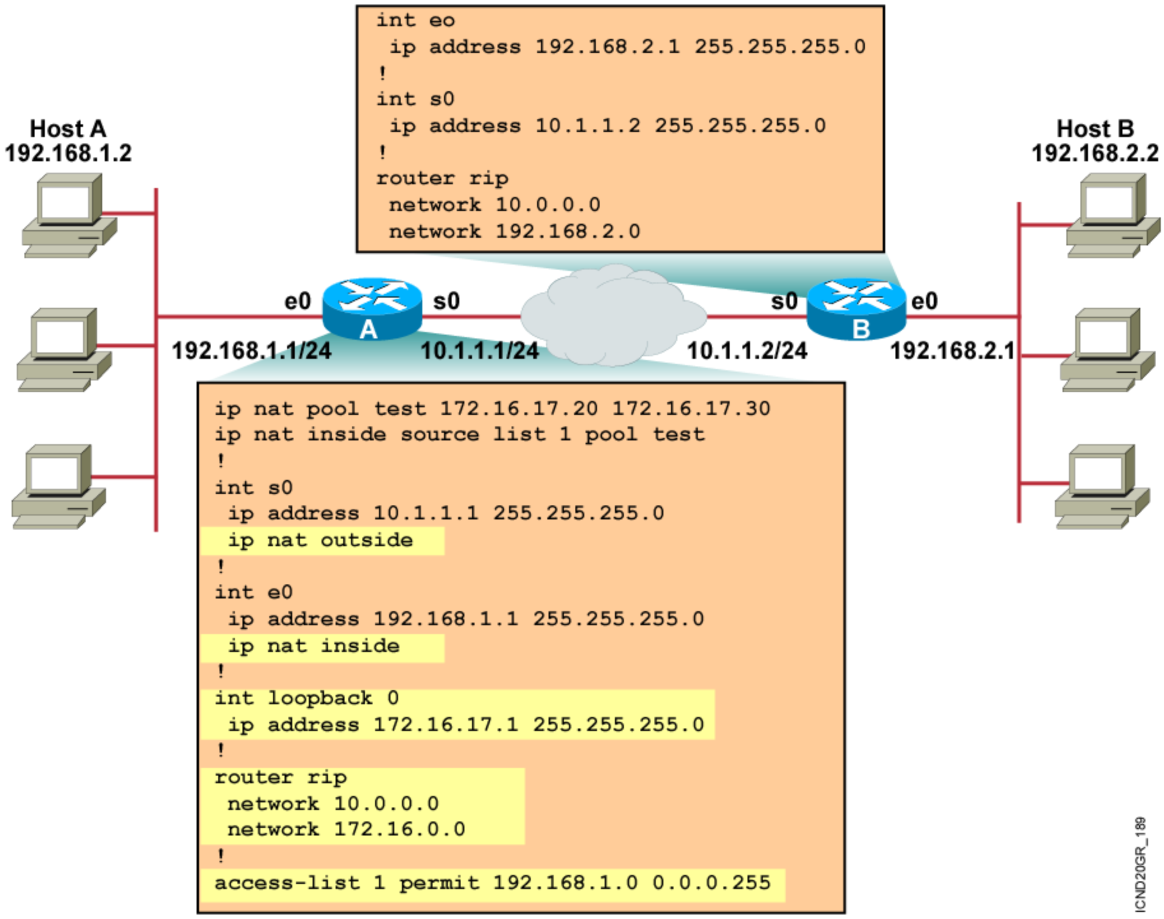
MONA#show ip nat translations
*Displays active translations
MONA#show ip nat translation

```
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.131.1       10.10.10.1        ---                ---
```

MONA#show ip nat statistics
***Displays translation statistics**

```
MONA#show ip nat statistics
    Total active translations: 1 (1 static, 0 dynamic; 0 extended)
    Outside interfaces:
    Ethernet0, Serial2.7
    Inside interfaces:
    Ethernet1
    Hits: 5  Misses: 0
```

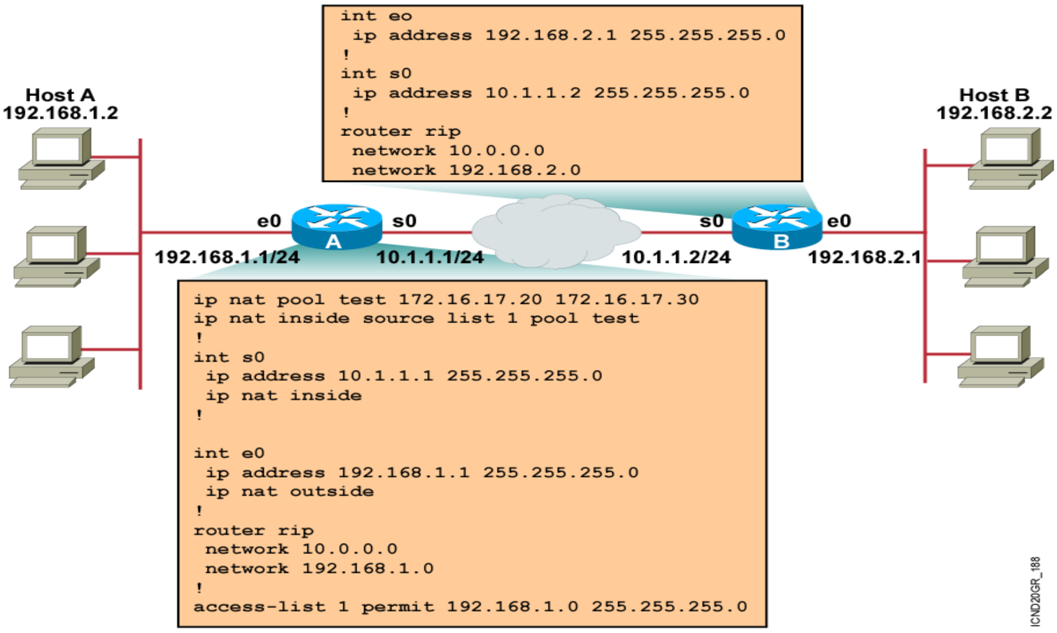
Sample Problem: Cannot Ping Remote Host



```
int eo
 ip address 192.168.2.1 255.255.255.0
!
int s0
 ip address 10.1.1.2 255.255.255.0
!
router rip
 network 10.0.0.0
 network 192.168.2.0
```

```
ip nat pool test 172.16.17.20 172.16.17.30
ip nat inside source list 1 pool test
!
int s0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
int e0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
int loopback 0
 ip address 172.16.17.1 255.255.255.0
!
router rip
 network 10.0.0.0
 network 172.16.0.0
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

New Configuration



```
int eo
 ip address 192.168.2.1 255.255.255.0
!
int s0
 ip address 10.1.1.2 255.255.255.0
!
router rip
 network 10.0.0.0
 network 192.168.2.0
```

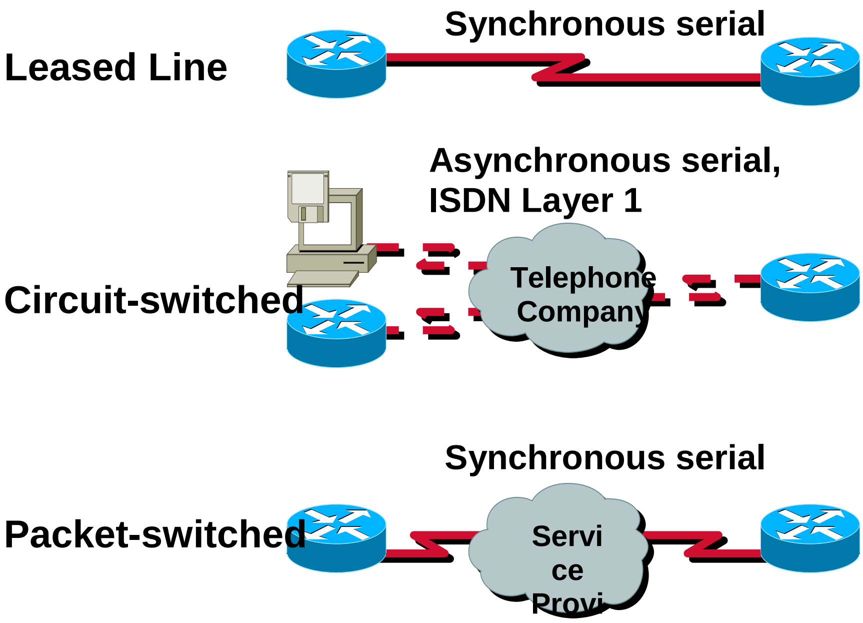
```
ip nat pool test 172.16.17.20 172.16.17.30
ip nat inside source list 1 pool test
!
int s0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!

int e0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
router rip
 network 10.0.0.0
 network 192.168.1.0
!
access-list 1 permit 192.168.1.0 255.255.255.0
```

Using the debug ip nat Command

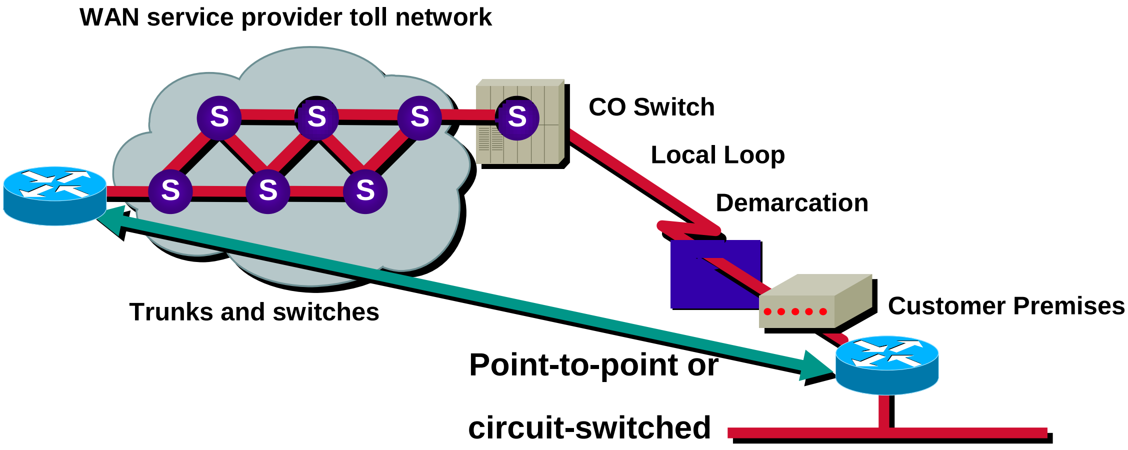
```
MONA#debug ip nat
 NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
         NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
         NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
         NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
         NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
         NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
         NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
         NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

WAN

WAN Connection Types

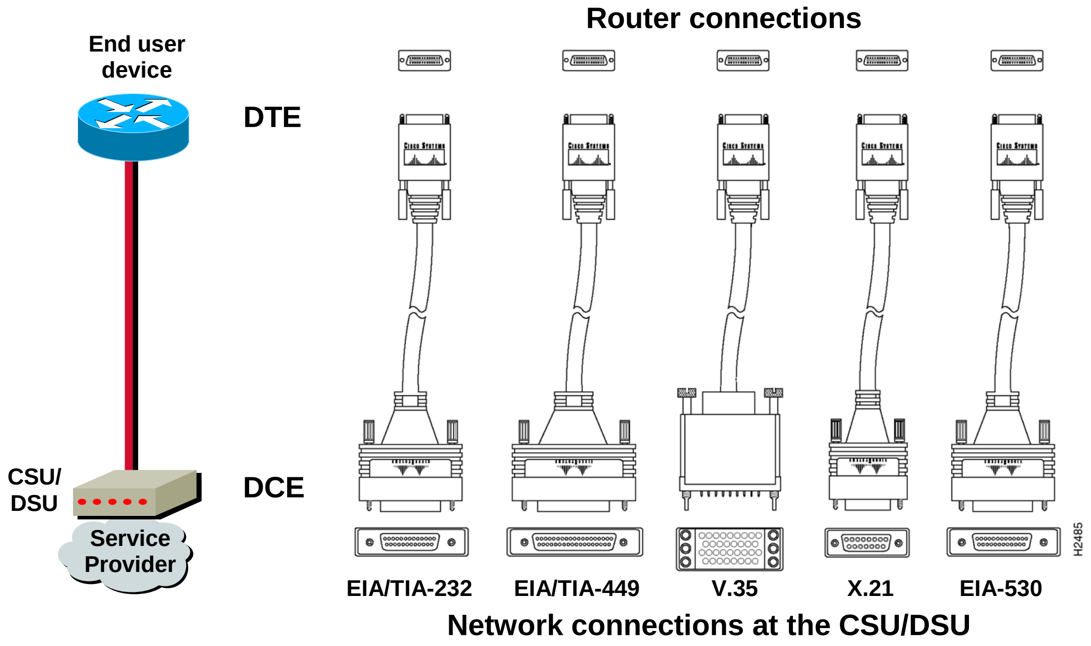


Interfacing WAN Service Providers

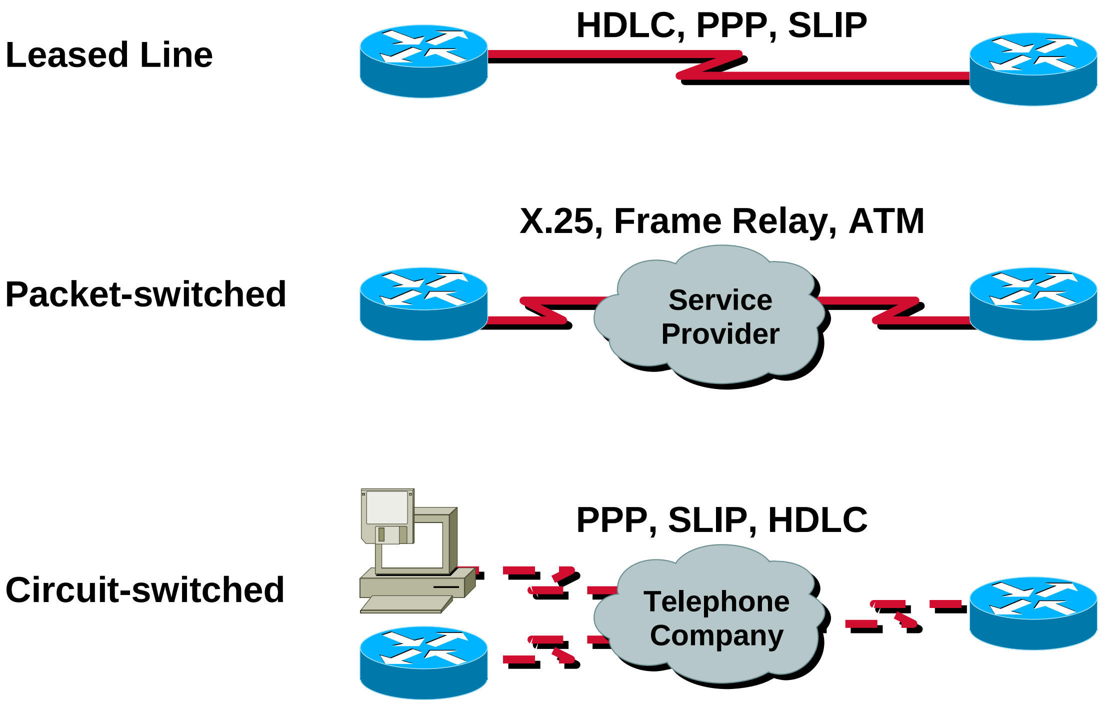


Provider assigns connection parameters to subscriber

Serial Point-to-Point Connections



Typical WAN Encapsulation Protocols



HDLC Frame Format

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag

*Cisco’s HDLC has a proprietary data field to support multiprotocol environments

HDLC

Flag	Address	Control	Data	FCS	Flag

*Supports only single protocol environments

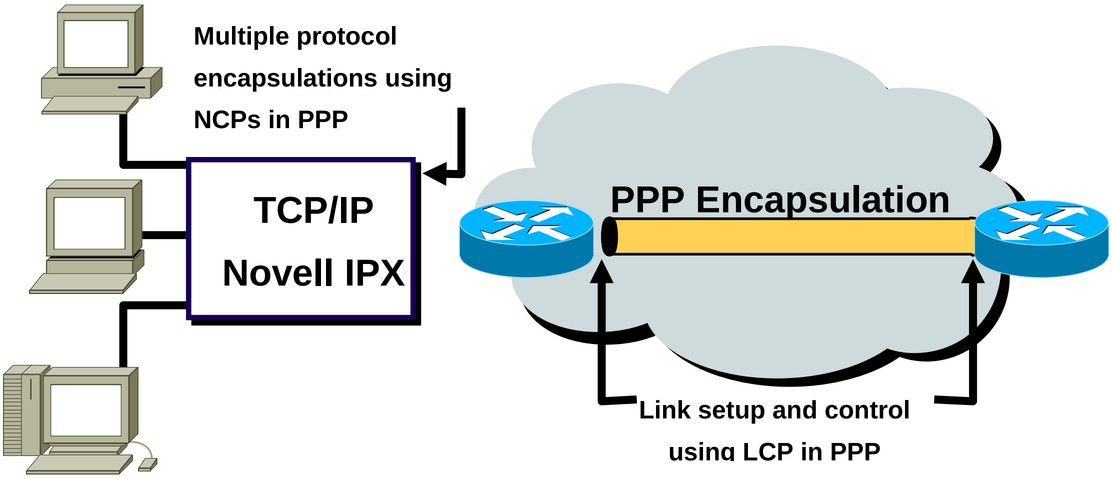
HDLC Command

MONA(config-if)#encapsulation hdlc

*Enable hdlc encapsulation

*HDLC is the default encapsulation on synchronous serial interfaces

An Overview of PPP



Multiple protocol encapsulations using NCPs in PPP

TCP/IP

Novell IPX

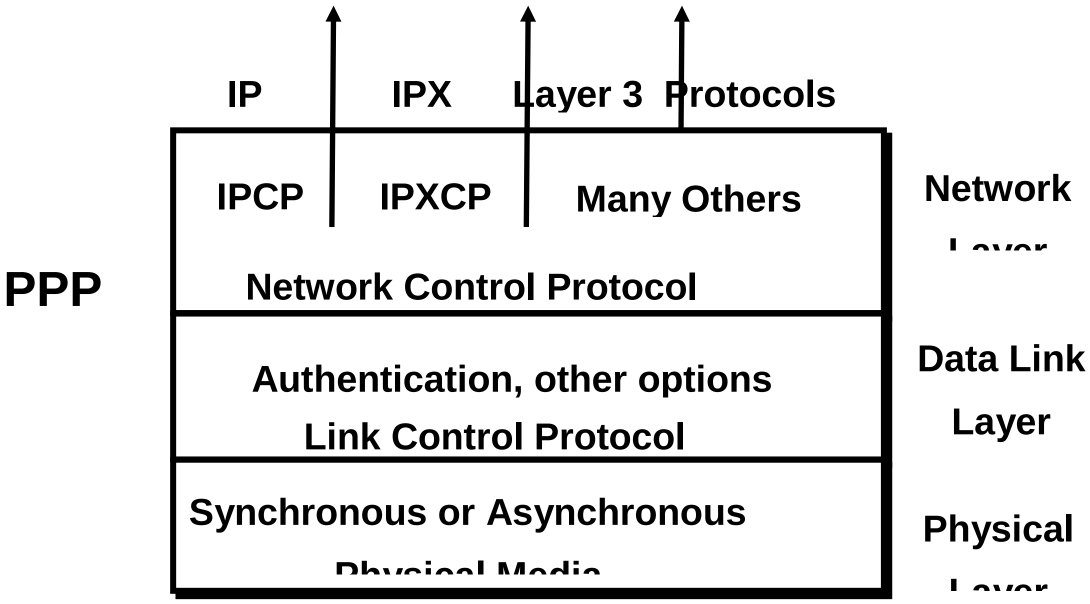
PPP Encapsulation

Link setup and control using LCP in PPP

*PPP can carry packets from several protocol suites using Network Control Programs

*PPP controls the setup of several link options using LCP

Layering PPP Elements



IP IPX Layer 3 Protocols

PPP

IPCP IPXCP Many Others

Network Control Protocol

Network Layer

Authentication, other options

Link Control Protocol

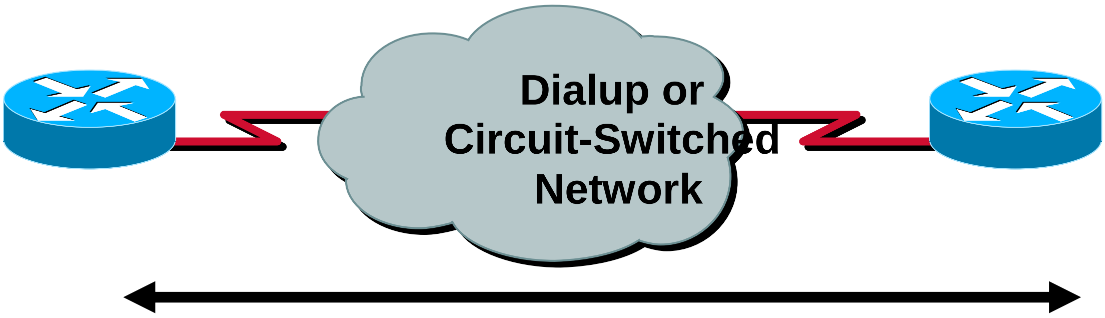
Data Link Layer

Synchronous or Asynchronous Physical Media

Physical Layer

PPP—A data link with network-layer services

PPP Authentication Overview



Dialup or Circuit-Switched Network

PPP Session Establishment

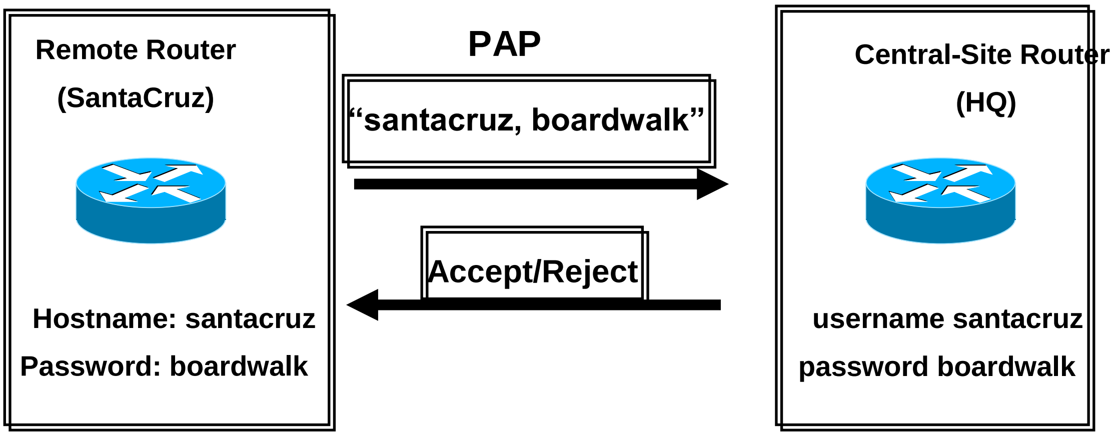
1 Link Establishment Phase

2 Optional Authentication Phase

3 Network-Layer Protocol Phase

Two PPP authentication protocols: PAP and CHAP

Selecting a PPP Authentication Protocol



Remote Router (SantaCruz)

PAP

“santacruz, boardwalk”

Accept/Reject

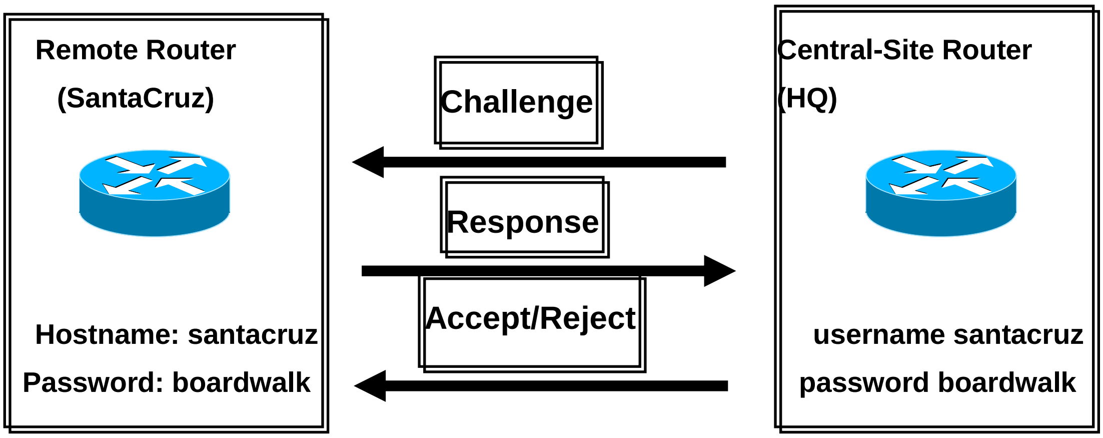
Central-Site Router (HQ)

Hostname: santacruz
Password: boardwalk

username santacruz
password boardwalk

*Passwords sent in clear text
*Peer in control of attempts

Selecting a PPP Authentication Protocol (cont.)



Remote Router (SantaCruz)

Challenge

Response

Accept/Reject

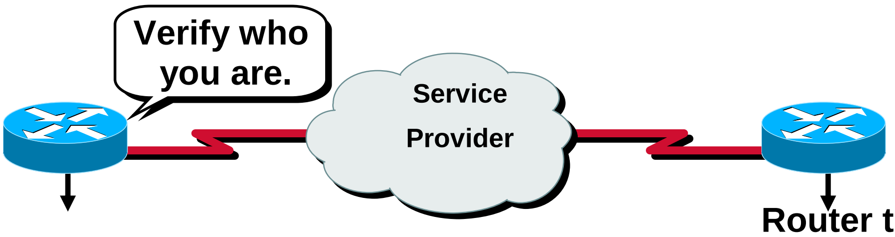
Central-Site Router (HQ)

Hostname: santacruz
Password: boardwalk

username santacruz
password boardwalk

Use “secret” known only to authenticator and peer

Configuring PPP and Authentication Overview



Verify who you are.

Service Provider

Authenticating Router
(The router that received the call.)

Router to Be Authenticated
(The router that initiated the call.)

Enabling PPP

☑ ppp encapsulation

Enabling PPP Authentication

☑ hostname
☑ username / password
☑ ppp authentication

Enabling PPP

☑ ppp encapsulation

☑ hostname
☑ username / password
☑ ppp authentication

Configuring PPP

MONA(config-if)#encapsulation ppp
Enable PPP encapsulation

Configuring PPP Authentication

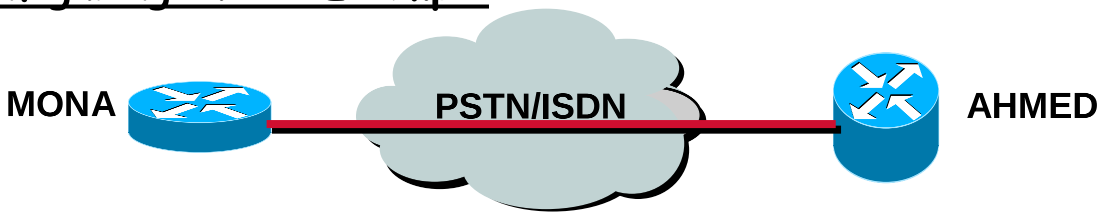
MONA(config)#hostname *name*

*Assigns a host name to your router
MONA(config)#username *name* password *password*
*Identifies the username and password of authenticating router

Configuring PPP Authentication(cont.)

MONA(config-if)#ppp authentication
{chap | chap pap | pap chap | pap}
Enables PAP and/or CHAP authentication

Configuring CHAP Example



```
hostname MONA
username right password 2011
!
int serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

```
hostname AHMED
username left password 1977
!
int serial 0
 ip address 10.0.1.2 255.255.255.0
 encapsulation ppp
 ppp authentication CHAP
```

Verifying HDLC and PPP Encapsulation Configuration

```
MONA#show interface s0
        Serial0 is up, line protocol is up
          Hardware is HD64570
          Internet address is 10.140.1.2/24
          MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
          Encapsulation PPP, loopback not set, keepalive set (10 sec)
          LCP Open
          Open: IPCP, CDPCP
          Last input 00:00:05, output 00:00:05, output hang never
          Last clearing of "show interface" counters never
          Queueing strategy: fifo
          Output queue 0/40, 0 drops; input queue 0/75, 0 drops
          5 minute input rate 0 bits/sec, 0 packets/sec
          5 minute output rate 0 bits/sec, 0 packets/sec
             38021 packets input, 5656110 bytes, 0 no buffer
             Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
             0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
             38097 packets output, 2135697 bytes, 0 underruns
             0 output errors, 0 collisions, 6045 interface resets
             0 output buffer failures, 0 output buffers swapped out
             482 carrier transitions
             DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

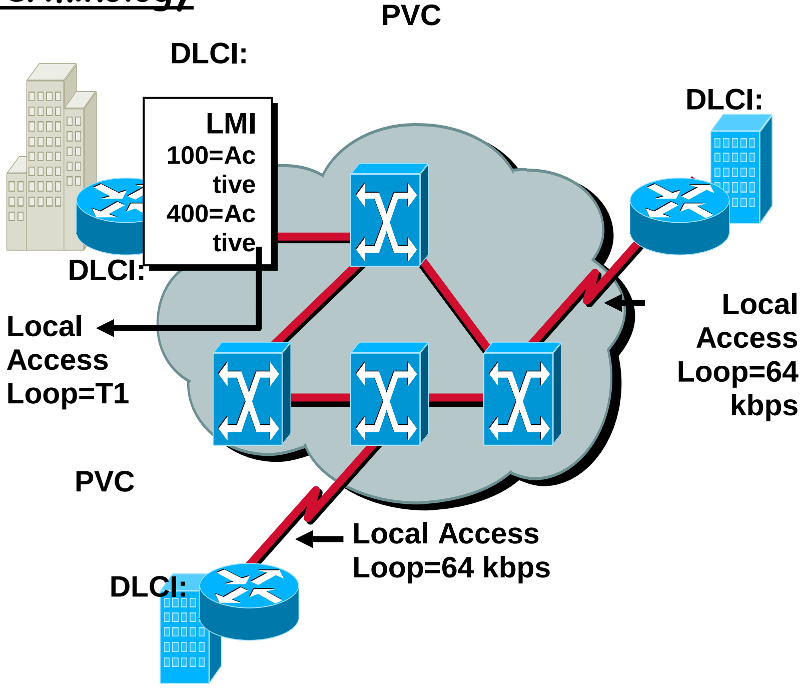
Verifying PPPAuthentication with the debug ppp authentication Command

```
4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
4d20h: Se0 PPP: Treating connection as a dedicated line
4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from ”left"
4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from ”right"
4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from ”left"
4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from ”right"
4d20h: Se0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0 CHAP: I SUCCESS id 3 len 4
4d20h: dialer Protocol up for Se0
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
```

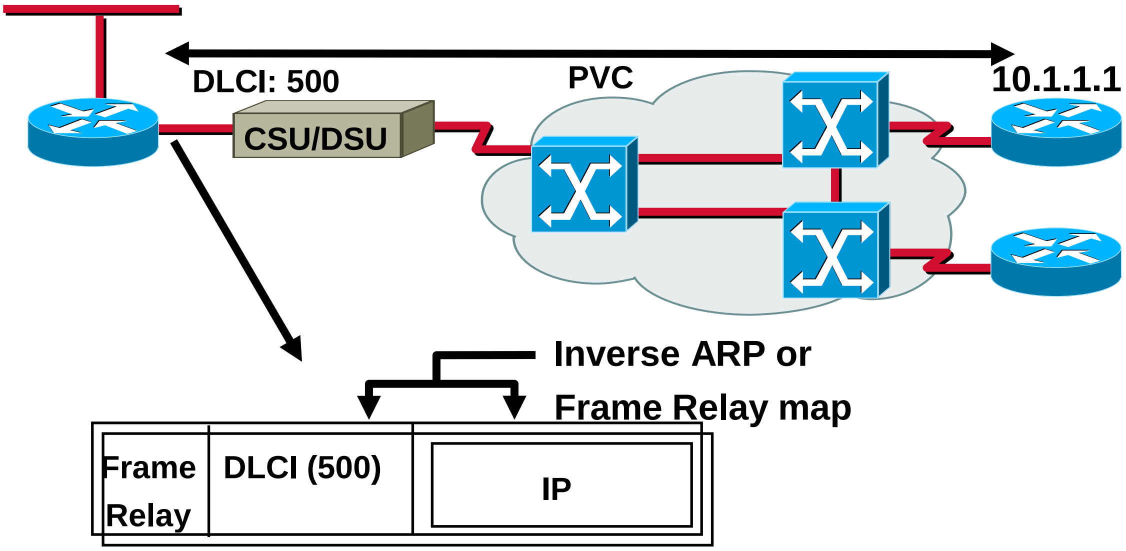
Frame Relay Stack

OSI Reference Model	Frame Relay
Application	
Presentation	
Session	
Transport	
Network	IP/IPX/AppleTalk, etc.
Data Link	Frame Relay
Physical	EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530

Frame Relay Terminology

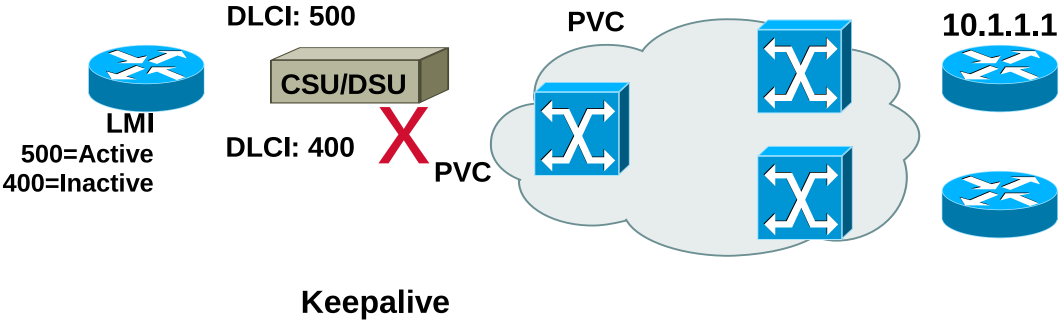


Frame Relay Address Mapping



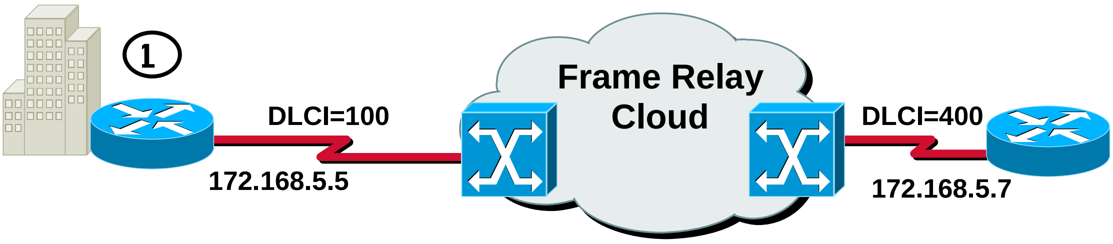
*Get locally significant DLCIs from provider
*Map your network addresses to DLCIs

Frame Relay Signaling

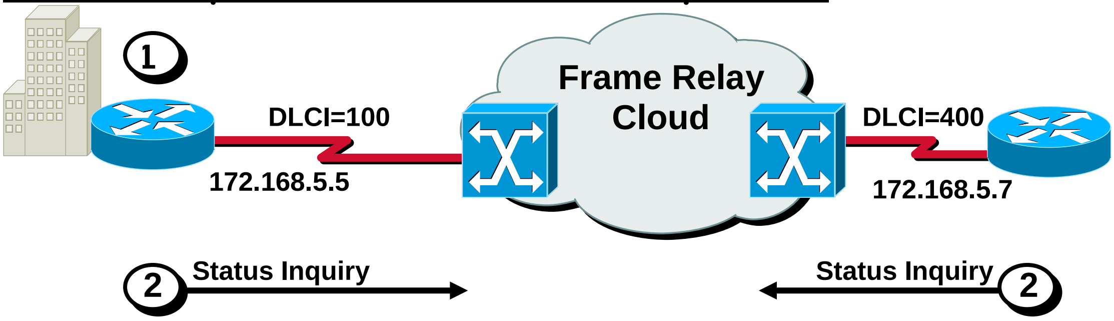


Cisco supports three LMI standards:
*Cisco
*ANSI T1.617 Annex D
*ITU-T Q.933 Annex A

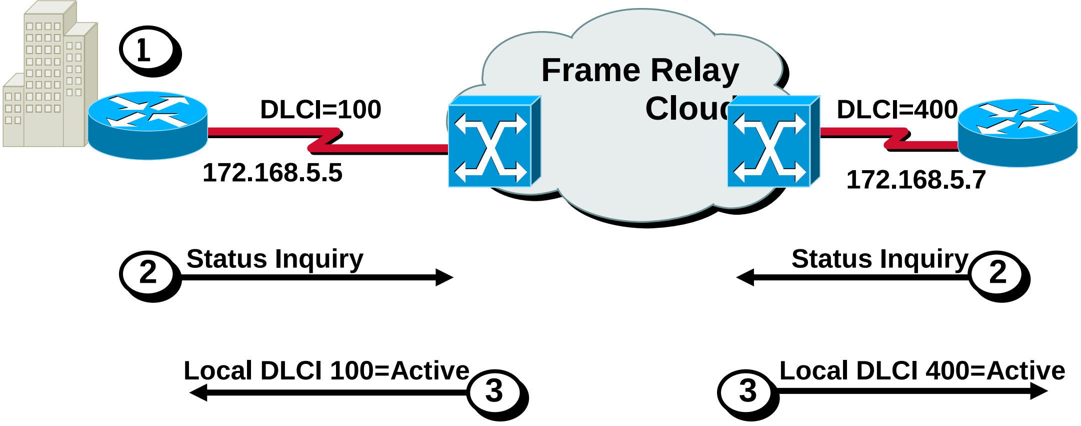
Frame Relay Inverse ARP and LMI Operation



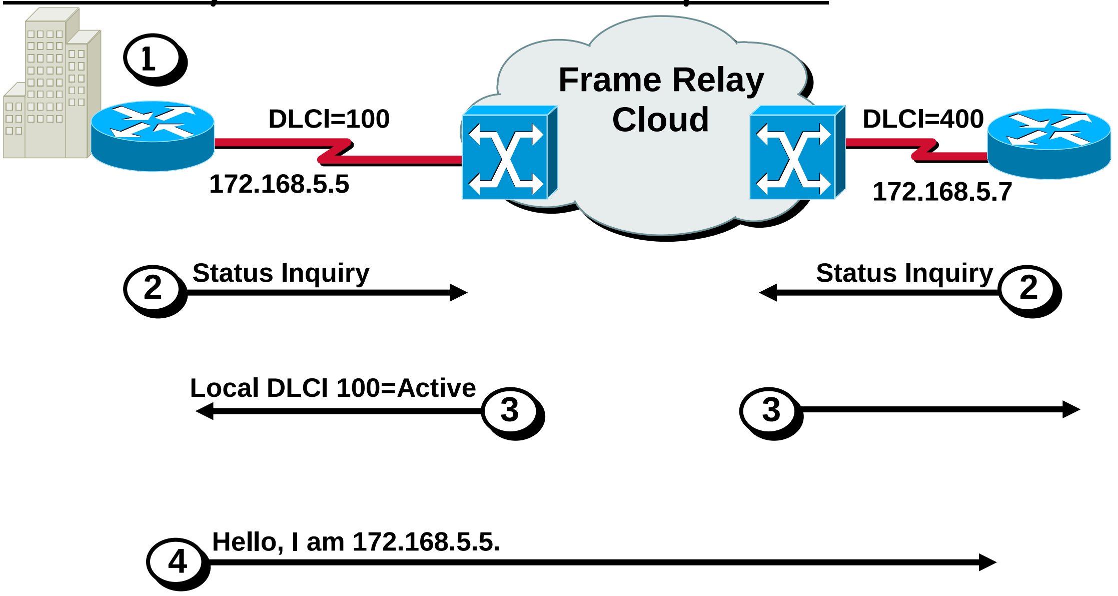
Frame Relay Inverse ARP and LMI Operation



Frame Relay Inverse ARP and LMI Operation



Frame Relay Inverse ARP and LMI Operation



Frame Relay Cloud

DLCI=100

172.168.5.5

DLCI=400

172.168.5.7

1

2 Status Inquiry

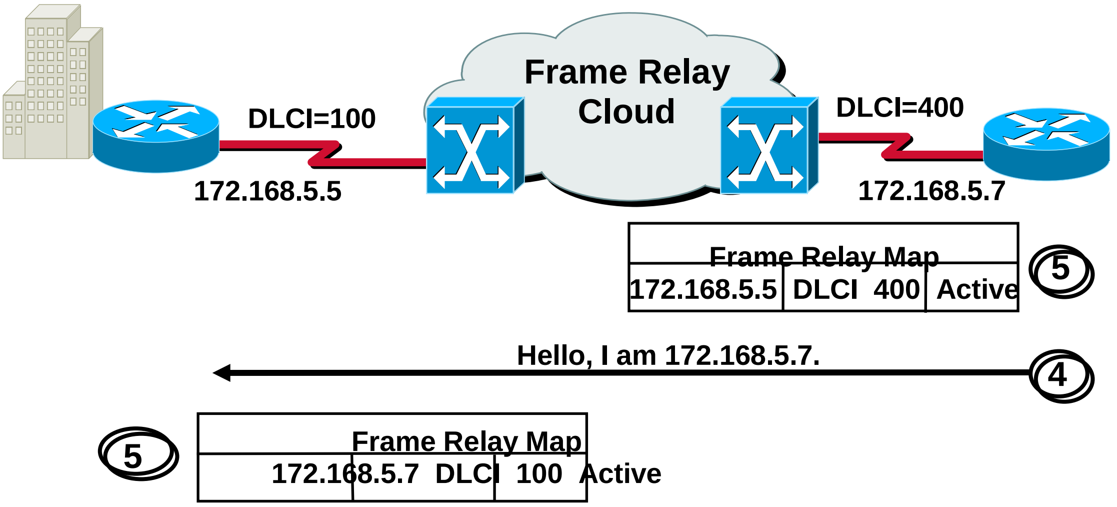
Status Inquiry 2

Local DLCI 100=Active 3

3

4 Hello, I am 172.168.5.5.

Frame Relay Inverse ARP and LMI Operation (cont.)



Frame Relay Cloud

DLCI=100

172.168.5.5

DLCI=400

172.168.5.7

Frame Relay Map

172.168.5.5	DLCI 400	Active

5

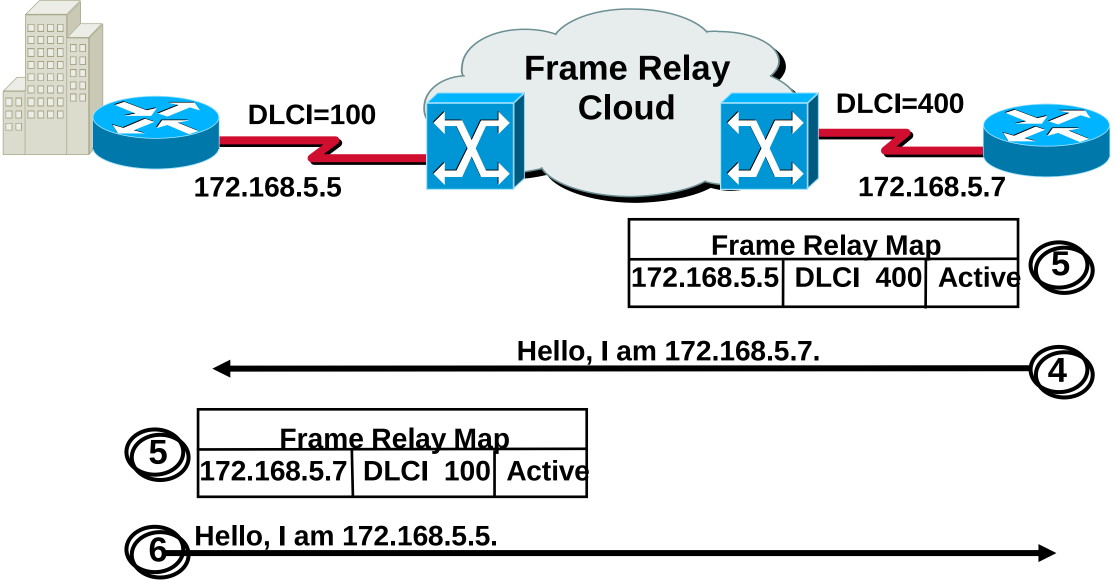
Hello, I am 172.168.5.7. 4

5

Frame Relay Map

172.168.5.7 DLCI 100 Active

Frame Relay Inverse ARP and LMI Operation (cont.)



Frame Relay Cloud

DLCI=100

172.168.5.5

DLCI=400

172.168.5.7

Frame Relay Map

172.168.5.5	DLCI 400	Active

5

Hello, I am 172.168.5.7. 4

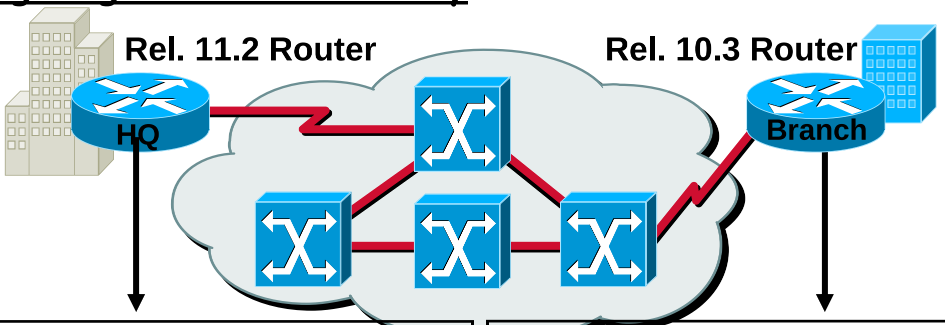
5

Frame Relay Map

172.168.5.7	DLCI 100	Active

6 Hello, I am 172.168.5.5.

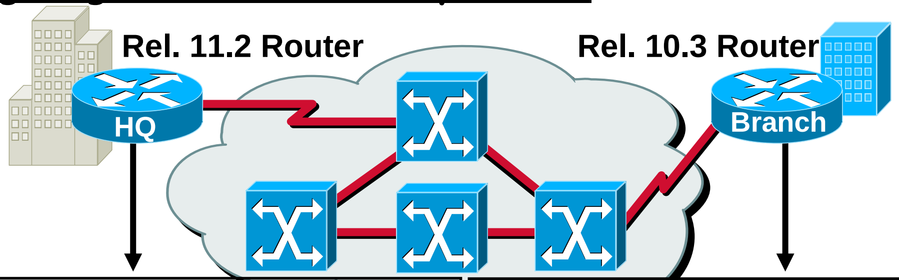
Configuring Basic Frame Relay



```
interface Serial1
 ip address 10.16.0.1 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
```

```
interface Serial1
 ip address 10.16.0.2 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
 frame-relay lmi-type ansi
```

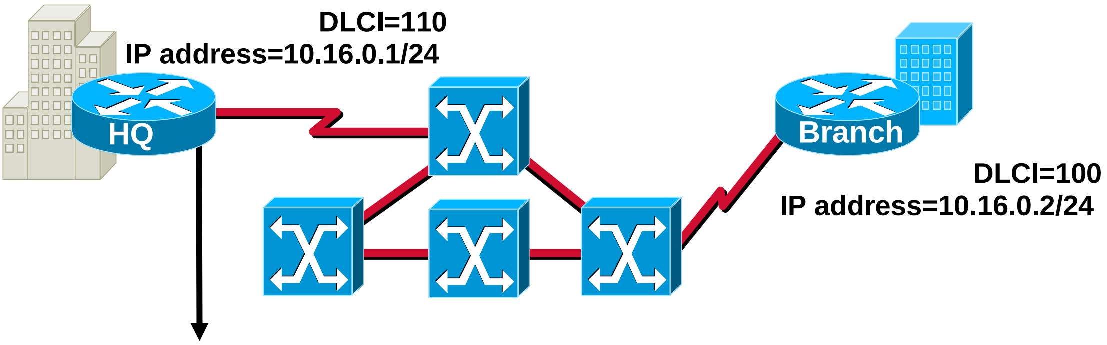
Configuring Basic Frame Relay (cont.)



```
interface Serial1
 ip address 10.16.0.1 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
```

```
interface Serial1
 ip address 10.16.0.2 255.255.255.0
 encapsulation frame-relay
 bandwidth 64
 frame-relay lmi-type ansi
```

Configuring a Static Frame Relay Map



```
interface Serial1
ip address 10.16.0.1 255.255.255.0
encapsulation frame-relay
bandwidth 64
frame-relay map ip 10.16.0.2 110 broadcast
```

Verifying Frame Relay Operation

```
MONA#show interface s0
        Serial0 is up, line protocol is up
          Hardware is HD64570
          Internet address is 10.140.1.2/24
          MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
          Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
          LMI enq sent  19, LMI stat recvd 20, LMI upd recvd 0, DTE LMI up
          LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
          LMI DLCI 1023  LMI type is CISCO  frame relay DTE
          FR SVC disabled, LAPF state down
          Broadcast queue 0/64, broadcasts sent/dropped 8/0, interface broadcasts 5
          Last input 00:00:02, output 00:00:02, output hang never
          Last clearing of "show interface" counters never
          Queueing strategy: fifo
          Output queue 0/40, 0 drops; input queue 0/75, 0 drops
          <Output omitted>
```

Displays line, protocol, DLCI, and LMI information

Verifying Frame Relay Operation (cont.)

MONA#show frame-relay lmi

```
         LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
         Invalid Unnumbered info 0 Invalid Prot Disc 0
         Invalid dummy Call Ref 0 Invalid Msg Type 0
         Invalid Status Message 0 Invalid Lock Shift 0
         Invalid Information ID 0 Invalid Report IE Len 0
         Invalid Report Request 0 Invalid Keep IE Len 0
         Num Status Enq. Sent 113100 Num Status msgs Rcvd 113100
         Num Update Status Rcvd 0 Num Status Timeouts 0
```

Displays LMI information

Verifying Frame Relay Operation (cont.)

```
MONA#show frame-relay pvc 100
        PVC Statistics for interface Serial0 (Frame Relay DTE)
        DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
          input pkts 28           output pkts 10          in bytes 8398
          out bytes 1198           dropped pkts 0          in FECN pkts 0
          in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
          in DE pkts 0            out DE pkts 0
          out bcast pkts 10        out bcast bytes 1198
          pvc create time 00:03:46, last time pvc status changed 00:03:47
        Displays PVC traffic statistics
```

Verifying Frame Relay Operation (cont.)

```
MONA#show frame-relay map
Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
                  broadcast,, status defined, active
```

Displays the route maps, either static or dynamic

Verifying Frame Relay Operation (cont.)

```
Router#show frame-relay map
        Serial0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic,
                  broadcast,, status defined, active
MONA#clear frame-relay-inarp
MONA#sh frame map
MONA#
```

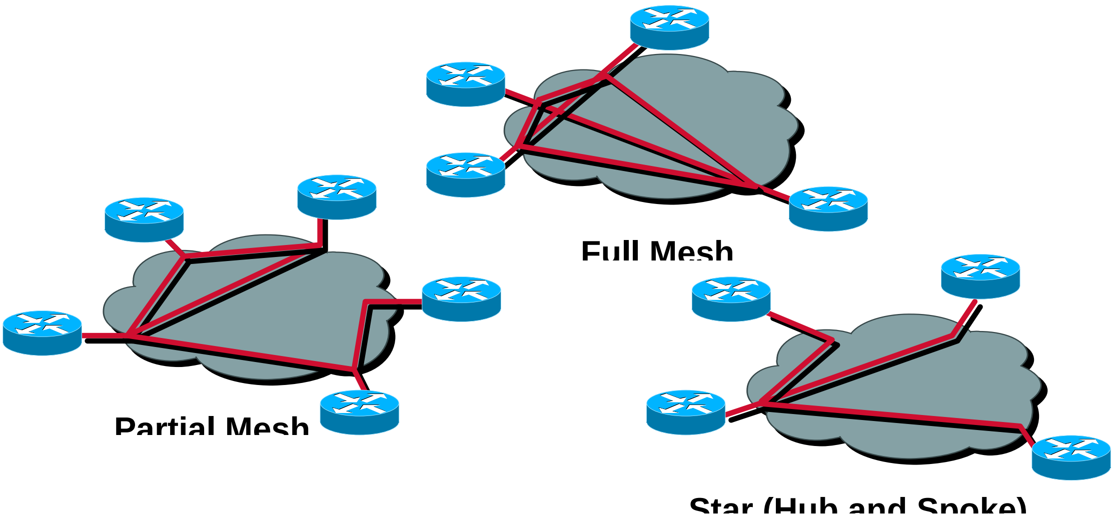
Clears dynamically created Frame Relay maps

Verifying Frame Relay Operation (cont.)

```
MONA#debug Frame lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router#
1w2d: Serial0(out): StEnq, myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0(in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0(out): StEnq, myseq 141, yourseen 140, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0(in): Status, myseq 142
1w2d: RT IE 1, length 1, type 0
1w2d: KA IE 3, length 2, yourseq 142, myseq 142
1w2d: PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
```

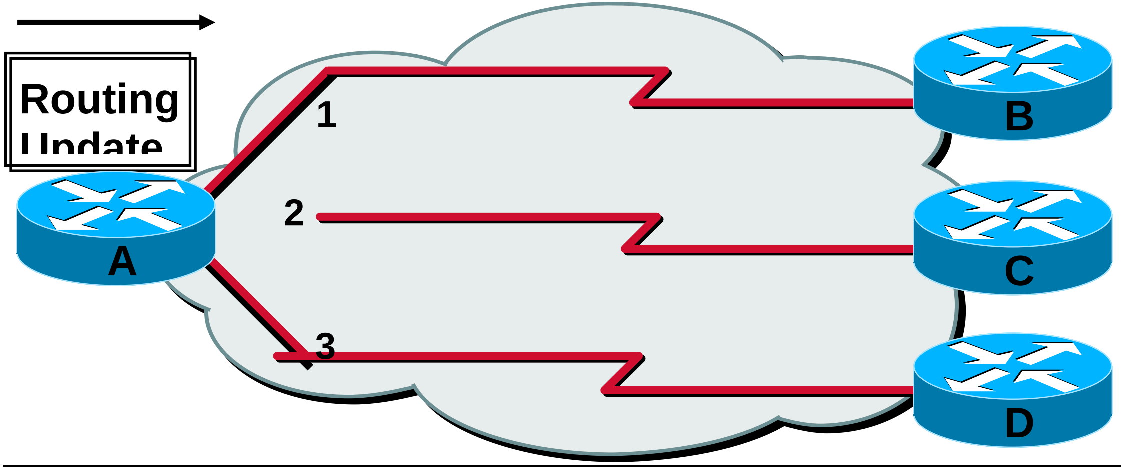
Displays LMI debug information

Selecting a Frame Relay Topology



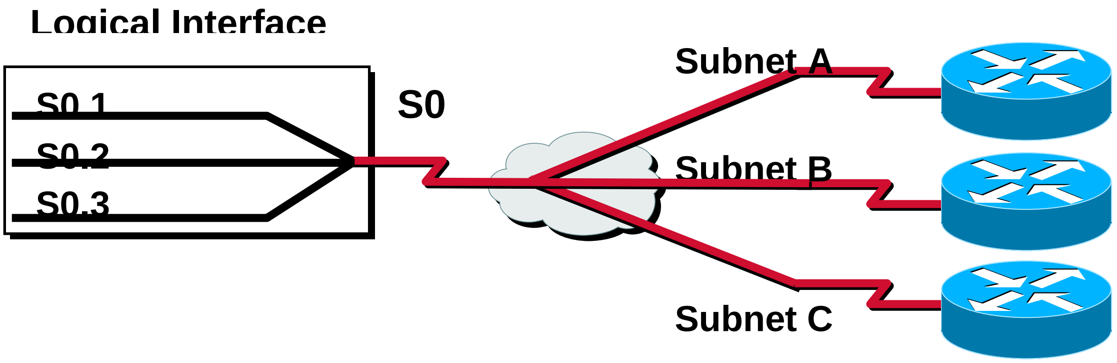
Frame Relay default: nonbroadcast, multiaccess (NMBA)

Reachability Issues with Routing Updates



Problem:
Broadcast traffic must be replicated for each active connection

Resolving Reachability Issues

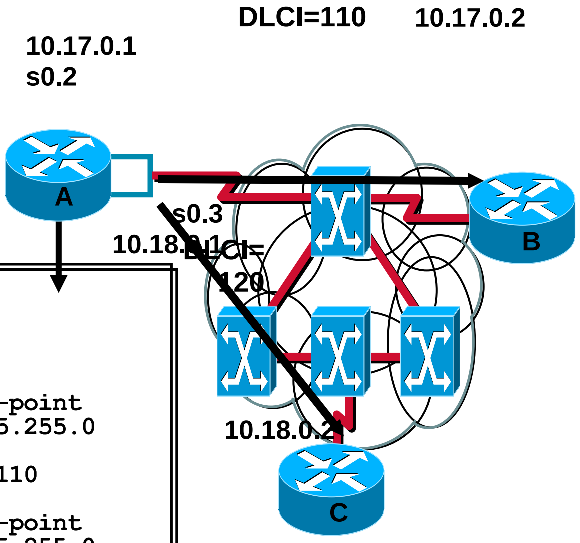


Solution:
*Split horizon can cause problems in NBMA environments
*Subinterfaces can resolve split horizon issues
*A single physical interface simulates multiple logical interfaces

Configuring Subinterfaces

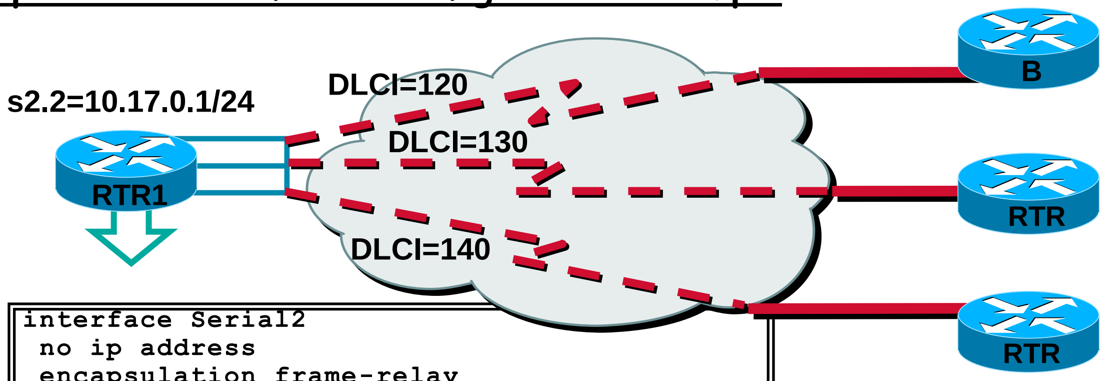
Point-to-Point
Subinterfaces act as leased line
Each point-to-point subinterface requires its own subnet
Applicable to hub and spoke topologies
Multipoint
Subinterfaces act as NBMA network so they do not resolve the split horizon issue
Can save address space because uses single subnet
Applicable to partial-mesh and full-mesh topology

Configuring Point-to-Point Subinterfaces



```
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.2 point-to-point
 ip address 10.17.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 110
!
interface Serial0.3 point-to-point
 ip address 10.18.0.1 255.255.255.0
 bandwidth 64
 frame-relay interface-dlci 120
!
```

Multipoint Subinterfaces Configuration Example



```
interface Serial2
 no ip address
 encapsulation frame-relay
!
interface Serial2.2 multipoint
 ip address 10.17.0.1 255.255.255.0
 bandwidth 64
 frame-relay map ip 10.17.0.2 120 broadcast
 frame-relay map ip 10.17.0.3 130 broadcast
 frame-relay map ip 10.17.0.4 140 broadcast
```

IPsec (Internet Protocol Security)

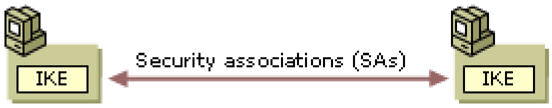
IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the Application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

Related glossary terms: managed security services (MSS), spam filter, port scan, unified threat management (UTM), script kiddy (or script kiddie), Snort, remote access, risk analysis, malware (malicious software), vulnerability analysis (vulnerability assessment)

Internet Key Exchange

Before secured data can be exchanged, a security agreement between the two computers must be established. In this security agreement, called a security association (SA), both agree on how to exchange and protect information, as shown in the following illustration.



To build this agreement between the two computers, the IETF has established a standard method of security association and key exchange resolution named Internet Key Exchange (IKE) which:

*Centralizes security association management, reducing connection time.

*Generates and manages shared, secret keys that are used to secure the information.

This process not only protects communication between computers, it also protects remote computers that request secure access to a corporate network. In addition, this process works whenever the negotiation for the final destination computer (endpoint) is performed by a security gateway.

Security association (SA) defined

A security association (SA) is the combination of a negotiated key, security protocol, and security parameters index (SPI), which together define the security used to protect the communication from sender to receiver. The SPI is a unique, identifying value in the SA that is used to distinguish among multiple security associations that exist at the receiving computer. For example, multiple associations might exist if a computer is securely communicating with multiple computers at the same time. This is a common occurrence when the computer is a file server or a remote access server that serves multiple clients. In these situations, the receiving computer uses the SPI to determine which SA is used to process the incoming packets.

Phase I or main mode SA

In order to ensure successful and secure communication, IKE performs a two-phase operation. Confidentiality and authentication are ensured during each phase by the use of encryption and authentication algorithms that are agreed upon by the two computers during security negotiations. With the duties split between two phases, key creation can be rapidly accomplished.

During the first phase, the two computers establish a secure, authenticated channel. This is called the phase I or main mode SA. IKE automatically provides necessary identity protection during this exchange.

Phase I or main mode negotiation

The following are the steps that comprise a main mode negotiation.

1/Policy negotiation

The following four mandatory parameters are negotiated as part of the main mode SA:

The encryption algorithm (DES or 3DES)

*The integrity algorithm (MD5 or SHA1)

*The Diffie-Hellman group to be used for the base keying material: Group 1 (768 bits of keying material) Group 2 (1,024 bits), or Group 2048 (2,048 bits)

*The authentication method (Kerberos V5, certificate, or preshared key authentication)

If certificates or preshared keys are used for authentication, the computer identity is protected. If Kerberos V5 authentication is used, the computer identity is unencrypted until encryption of the entire identity payload takes place during authentication.

Important

For enhanced security, do not use Diffie-Hellman Group 1. For maximum security, use Group 2048 whenever possible. Use Group 2 when required for interoperability with Windows 2000 and Windows XP.

For more information about Diffie-Hellman groups, see Key exchange methods.

For more information about preshared key authentication, see Preshared key authentication.

Diffie-Hellman exchange (of public values)

At no time are actual keys exchanged. Only the base information required by the Diffie-Hellman key determination algorithm to generate the shared, secret key is exchanged. After this exchange, the IKE service on each computer generates the master key that is used to protect authentication.

1/Authentication

To prevent a successful man-in-the-middle attack, the computers attempt to authenticate the Diffie-Hellman key exchange. Without successful authentication, communication will not proceed. The master key is used, in conjunction with the negotiation algorithms and methods, to authenticate identities. The entire identity payload is hashed and encrypted using the keys generated from the Diffie-Hellman exchange in the second step. The payload includes the identity type (for authentication), port, and protocol. IPSec uses the following identity types for authentication: For certificate authentication, the certificate distinguished name and general name; for Kerberos V5 and preshared key authentication, IPv4 addresses, the fully qualified domain name (FQDN) of the computer, and FQDN of the user. The identity payload, regardless of which authentication method is used, is protected from both modification and interpretation.

The sender presents an offer for a potential security association to the receiver. The responder cannot modify the offer. Should the offer be modified, the initiator rejects the responder's message. The responder sends either a reply accepting the offer or a reply with alternatives.

Messages sent during this phase have an automatic retry cycle that is repeated five times. If a response is received before the retry cycle ends, standard SA negotiation begins. If allowed by IPSec policy, unsecured communications will begin after a brief interval. If unsecured communications begin, after five minutes of idle time (during which no messages are sent), secured communication negotiation is attempted the next time messages are sent. If messages are sent continuously, the communication remains unsecured during the lifetime set for the main mode policy. After the policy time has elapsed, a new secured communication negotiation attempt is made.

There is no preset limit to the number of exchanges that can take place. The number of SAs established is only limited by system resources. When estimating the number of SAs that can be established without significantly degrading computer performance, consider the CPU processing strength and RAM of the computer, the lifetime of the SA, and how much traffic is being sent over the SAs.

For more information about unsecured communications, see Filter action.

Phase II or quick mode SA

In this phase, SAs are negotiated on behalf of the IPSec driver.

Phase II or quick mode negotiation

The following are the steps that comprise a quick mode negotiation.

1/Policy negotiation occurs.

The IPSec computers exchange the following requirements for securing the data transfer:

*The IPSec protocol (AH or ESP)

*The hash algorithm for integrity and authentication (MD5 or SHA1)

*The algorithm for encryption, if requested (3DES or DES)

A common agreement is reached, and two SAs are established. One SA is for inbound communication and the other is for outbound communication.

1/Session key material is refreshed or exchanged.
IKE refreshes the keying material and new shared keys are generated for packet integrity, authentication, and encryption (if negotiated). If rekeying is required, either a second Diffie-Hellman exchange (as described in main mode negotiation) occurs, or a refresh of the original Diffie-Hellman key is used.

1/The SAs and keys, along with the SPI, are passed to the IPSec driver.

The second negotiation of security settings and keying material (for the purpose of securing data) is protected by the main mode SA. As the first phase provided identity protection, the second phase provides protection by refreshing the keying material prior to sending data. IKE can accommodate a key exchange payload for an additional Diffie-Hellman exchange if a rekey is necessary--that is, master key perfect forward secrecy (PFS) is enabled. Otherwise, IKE refreshes the keying material from the Diffie-Hellman exchange completed in main mode.

Quick mode results in a pair of security associations, each with its own SPI and key. One SA is used for inbound communication, and the other for outbound communication.

Notes

*Although there are two separate quick mode SAs established, IP Security Monitor only displays a single quick mode SA.

*Computers running Windows 2000 must have the High Encryption Pack or Service Pack 2 (or later) installed in order to use the 3DES algorithm. If a computer running Windows 2000 receives a 3DES setting, but does not have the High Encryption Pack or Service Pack 2 (or later) installed, the 3DES setting in the security method is set to the weaker DES, to provide some level of confidentiality for communication, rather than blocking all communication. However, you should only use DES as a fallback option if not all computers in your environment support the use of 3DES. Computers running Windows XP or a Windows Server 2003 operating system support 3DES and do not require installation of the High Encryption Pack.

The retry algorithm for a message is similar to the process described in main mode negotiation. However, if this process times out for any reason during the second or higher negotiation off of the same main mode SA, a renegotiation of the main mode SA is attempted. If a message for this phase is received without an established main mode SA, it is rejected.

Using a single main mode SA for multiple quick mode SA negotiations increases the speed of the process. As long as the main mode SA does not expire, renegotiation and reauthentication are not necessary. The number of quick mode SA negotiations that can be performed is determined by IPSec policy settings.

Note

*Excessive rekeying off of the same main mode SA might make the shared, secret key vulnerable to a known plaintext attack. A known plaintext attack is a sniffer attack in which the attacker attempts to determine the encryption key from encrypted data based on known plaintext.

SA lifetimes

The main mode SA is cached to allow multiple quick mode SA negotiations (unless master key PFS is enabled). When a key lifetime is reached for the master or session key, the SA is renegotiated. In addition, the key is refreshed or regenerated.

When the default time-out period elapses for the main mode SA, or the master or session key lifetime is reached, a delete message is sent to the responder. The IKE delete message tells the responder to expire the main mode SA. This prevents additional new quick mode SAs from being created from the expired main mode SA. IKE does not expire the quick mode SA, because only the IPSec driver contains the number of seconds or bytes that have passed to reach the key lifetime.

Use caution when setting very different key lifetimes for master and session keys. For example, setting a master key lifetime of eight hours and a session key lifetime of two hours might leave a quick mode SA in place for almost two hours after the main mode SA has expired. This occurs when the quick mode SA is generated shortly before main mode SA expiration.

It is generally recommended that all of the IKE settings (for example, master key PFS and key lifetime) and security methods remain at their defaults to avoid unnecessary administrative overhead. This provides a standard (medium) level of security. If your security plan calls for a high level of security, you should consider modifying the default security methods.

ESP, Encapsulating Security Payload

Description:

Protocol suite:	IPSec.TCP/IP
:Protocol type	ransport layer protocol.
Protocol:IP	50.
subtype:MIME	
MIBs:SNMP	
:Working groups	, IP Security Protocol.ipsec , IP Security Maintenance and Extensions.ipsecme , Multicast Security.msec
Links:	

ESP will function with both the IPv4 and IPv6 protocols.

ESP supports two modes of operation, tunnel mode and transport mode.

RFC 4303:

The ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with AH, or in a nested fashion.

Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.

MAC header	| IPv6 headerIPv4	ESP header	Data :::

ESP header:

Security Parameters Index		
Sequence number		
:::Payload data		
::Padding	Pad length	Next header
:::Authentication data		

SPI, Security Parameters Index. 32 bits.
An arbitrary value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the SA for this datagram. The set of SPI values in the range 1 through 255 are reserved for future use. A reserved SPI value will not normally be assigned by IANA unless the use of the assigned SPI value is specified in an RFC. It is ordinarily selected by the destination system upon establishment of an SA. This field is mandatory. The value of zero is reserved for local, implementation- specific use and MUST NOT be sent on the wire. For example, a key management implementation MAY use the zero SPI value to mean "No Security Association Exists" during the period when the IPsec implementation has requested that its key management entity establish a new SA, but the SA has not yet been established.

Sequence number. 32 bits, unsigned.
This field contains a monotonically increasing counter value. It is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. Processing of this field is at the discretion of the receiver. The sender MUST always transmit this field, but the receiver need not act upon it. The sender's counter and the receiver's counter are initialized to 0 when an SA is established. The first packet sent using a given SA will have a Sequence number of 1. If anti-replay is enabled (the default), the transmitted Sequence number must never be allowed to cycle. Thus, the sender's counter and the receiver's counter MUST be reset (by establishing a new SA and thus a new key) prior to the transmission of the 2^32nd packet on an SA.

Payload data. Variable length.
Contains the data described by the *Next header* field. This field is mandatory and is an integral number of bytes in length. If the algorithm used to encrypt the payload requires cryptographic synchronization data, e.g., an Initialization Vector (IV), then this data MAY be carried explicitly in the *Payload data* field. Any encryption algorithm that requires such explicit, per-packet synchronization data MUST indicate the length, any structure for such data, and the location of this data as part of an RFC specifying how the algorithm is used with ESP. If such

synchronization data is implicit, the algorithm for deriving the data MUST be part of the RFC.

Padding. Variable length, 0 to 255 bytes.
Padding may be required, irrespective of encryption algorithm requirements, to ensure that the resulting ciphertext terminates on a 4 byte boundary. Specifically, the *Pad length* and *Next header* fields must be right aligned within a 4 byte word to ensure that the Authentication data field, if present, is aligned on a 4 byte boundary.

Pad length. 8 bits.
Specifies the size of the *Padding* field in bytes.

Next header. 8 bits.
An IPv4/IPv6 protocol number describing the format of the *Payload data* field.

Authentication data. Variable length.
Contains an ICV computed over the ESP packet minus the Authentication data. The length of the field is specified by the authentication function selected. This field is optional and is included only if the authentication service has been selected for the SA in question. The authentication algorithm specification MUST specify the length of the ICV and the comparison rules and processing steps for validation.

IPv6

Introduction to IPv6

Due to recent concerns over the impending depletion of the current pool of Internet addresses and the desire to provide additional functionality for modern devices, an upgrade of the current version of the Internet Protocol (IP), called IPv6, has been standardized. This new version, called IP version 6 (IPv6), resolves unanticipated IPv4 design issues and takes the Internet into the 21st Century.

This paper describes the problems of the IPv4 Internet and how they are addressed by IPv6, IPv6 addressing, the new IPv6 header and its extensions, the IPv6 replacements for the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP), neighboring node interaction, IPv6 address autoconfiguration, and IPv6 routing. This paper provides a foundation of Internet standards-based IPv6 concepts and is intended for network engineers and support professionals who are already familiar with basic networking concepts and TCP/IP.

TCP/IP v4 and v6

Windows Server 2008 and Windows Vista TCP/IP was completely redesigned to support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) to meet the connectivity and performance needs of today's varied networking environments and technologies.

These protocols provide IP addresses, the "phone numbers" for the Internet that are responsible for identifying computers and devices so that they can communicate.

IPv6 is designed to solve many of the problems of IPv4, including mobility, auto-configuration, and overall extensibility. IPv6 expands the address space on the Internet and supports a nearly unlimited number of devices that can be directly connected to the Internet.

Business Resources

IPv6 Support in Microsoft Products and Services
Case Study: How Microsoft IT has Deployed IPv6 on the Microsoft Corpnet
Development and Deployment of IPv6: Good for Internet, Technology
Enabling the Next Generation of Networking with End-to-End IPv6
Bechtel Well Positioned to Serve Customers by Using Microsoft and Cisco IPv6 Solution

Technical Resources for IPv4

- TCP/IP Registry Values for Microsoft Windows Vista and Windows Server 2008
- Windows Server 2008 TCP/IP Protocols and Services
- TCP Receive Window Auto-Tuning
- Receive-Side Scaling Enhancements in Windows Server 2008
- Explicit Congestion Notification (ECN) for TCP/IP
- Link-Local Multicast Name Resolution
- Strong and Weak Host Models

تطور مسيرة الحاسبات الآلية في السودان (١٩٦٧-١٩٨٤) :

لقد تم ادخال اول حاسوب في السودان وربما افريقيا والشرق الاوسط عام ١٩٦٧ وتم به تاسيس مركز الحاسب الالي بجامعة الخرطوم بغرض تدريب الطلاب والبحث العلمي والاستخدام الاداري ثم اعقب ذلك الادارة المركزية التي ادخلت الحاسوب في ادارة حسابات الزبائن في عام ١٩٦٨ وفي العام التالي ادخلت مصلحة الاحصاء الحاسوب للاستخدامات الاحصائية وظل الوضع علي ما هو عليه حتي السبعينات حيث ادخلت ادارة السكة الحديد ومصنع النسيج السوداني والياباني الحاسوب في ادارتها وفي عام ١٩٧٧ ادخل الحاسوب الي شعبة الاقتصاد القياسي بجامعة الخرطوم بنفس اغراض مركز الحاسب الالي اما خلال الاعوام ١٩٧٨ و١٩٧٩ و١٩٨٠ قد حدث تطور عجيب في استخدامات الحواسيب حيث ادخلت اكثر من خمسة عشر مؤسسة الحاسوب في ادارتها بسبب دخول حواسيب صغيرة عالية القدرة وسهلة الاستخدام ومدعومة ببرامج تطبيقية مناسبة وباسعار معقولة ومجدية نوعا ما وقد استمر هذا النوع من الحواسيب في الانتشار حتي منتصف الثمانينات حتي تجاوز عددها [١] .

مشكلات الحاسبات الآلية في السودان:

هنالك عده اسباب ادت الى عدم تطور استخدام الحاسب منها :

اولهما: محاربة الاداريين

والثاني: النقص في الكادر المؤهل من محللي النظم والمبرمجين

المؤسسات التي تستعمل الحاسب الالي في السودان

اسم المؤسسة	مكان التركيب	نوع الحاسب الالي	سنة التركيب	حجم الذاكرة	نوع التطبيقات	عدد ساعات الاستعمال
أ) أي س ال						
مصنع النسيج السوداني	الخرطوم	١٩٠٣	١٩٧٤	٤٨ ك ب	تجارى	٦
مصنع النسيج الياباني	الخرطوم	١٩٠٢	١٩٧٥	٤٨ ك ب	تجارى	الغي
السكة حديد	عطبرة	١٩٠٣	١٩٧٦	٤٨ ك ب	تجـــارى	٦
شعبة الاقتصاد القياسي	جامعة الخرطوم	١٩٠٣	١٩٧٧	٤٨ ك ب	وعلمي	٦
مصلحة الاحصاء	الخرطوم	ام اي ٢٩	١٩٨٤	ا م ب	علمـــي	٨
الخطـــوط الجويـــة	الخرطوم	ام اي ٢٩	١٩٨٤	٥٠٠ك ب	وتجارى	-
السودانية					علمي	

[١] * مجلة الدراسات السودانية- العدد الاول – المجلد السابع أغسطس ١٩٨٩م

					علمـــــــي وتجارى	
*** اي بي ام**						
الادارة المركزيـــــة للكهربـــــاء الخرطوم	٣٦٠/٢٠استبدلت ب ان سي ار٤٠٢٠ ١٩٦٨ ٦٤ ك تجارى ١٦					
مصلحة الاحصاء	الخرطوم	٣٦٠/٢٠ق ٣٠استبدلت ب اي س ال م اي ٥٢٩	١٩٦٩	٦٤ ك	علمي	
شل	الخرطوم	٣٦٠|/٣٠ استبدلت ب سيستم ٣٤	١٩٧٥	٦٤	تجارى	٦
بنك ابو ظبي	الخرطوم	سيستم ٣٤	١٩٨١	١٢٨ك	تجاري	٨
*** وانق (مؤسسة الوقيع)**						
شركة بيطار	الخرطوم	في بي ٢٢٠٠	١٩٧٨	٣٢ ك ب	تجارى	٨
البنك العالمي السوداني	الخرطوم	" " "	١٩٧٩	٦٤ ك ب	تجارى	٨
بنك النيلين	الخرطوم	ام في بي٢٢٠٠	١٩٧٩	٦٤ك ب	تجارى	٨
بنك الخرطوم	الخرطوم	" " "	١٩٧٩	٦٤ ك ب	تجارى	٨
شركة الروبي	الخرطوم	في بي ٢٢٠٠	١٩٨٠	٦٤ك ب	تجارى	٨
القوات المسلحة	الخرطوم	ام في بي٢٢٠٠	١٩٨١	٦٤ك ب	علمي وتجاري	٨
مطبعة التمدن	الخرطوم	،، ،،	١٩٨٢	٦٤ ك ب	تجاري	٨
جامعة الخرطوم	الخرطوم	في اس ١٠٠	١٩٨٤	اي بي ام	علمي وتجاري وتعلمي	١٢
البنك السعودي	الخرطوم	ام في بي	١٩٨٤	٦٤ ك ب	تجاري	٨
***أن سي آر** جامعة الخرطوم	الخرطوم	اليـــوت ٨٠٣ استبدلت بوانق في اس ١٠٠	١٩٦٧	٨ ك	علمي وتعلمي وتجاري	١٢
مصنع سكر كنانة	كنانة×	٢× اي ٩٠٢٠	١٩٧٨	٢٥٦ ك ب	تجاري	١٦
بنك الاعتماد	الخرطوم	آي ٩٠٢٠	١٩٧٨	١٢٨ ك ب	تجاري	٨
القوات المسلحة	الخرطوم	اي ٩١٠	١٩٧٩	-	تجاري	٦
مصـــنع نســيج النيـــل الازرق	ود مدني	،، ،،	١٩٨٠	١٢٠ ك	تجلري	٦

ماسبيو	عطبرة	٣× آي ٩٠١٠	١٩٨٠	٦٤ ك	تجاري	٨
بنك الاعتماد	امدرمان	آي ٩٠٢٠	١٩٨٠	١٢٨ ك	تجاري	٨
بنك الوحدة	الخرطوم	١٣ × آي ٩٠١٠	١٩٨٠	٦٤ ك	تجاريي	٨
بنك الاعتماد	بورتسودا	اي ٩٠١٠	١٩٨٠	٦٤ ك	تجاري	٨
بنك النيلين	الخرطوم	١٠× آي ٩٠١٠	١٩٨٠	٦٤ ك	تجاري	٨
بنك الشرق الاوسط	الخرطوم	اي ٩٠٢٠	١٩٨٠	١٢٨ ك	تجاري	٨
خدمات الجزيرة	الخرطوم	٤×٩٠١٠	١٩٨١	٦٤	تجاري	٦
بنك الشعب التعاوني	الخرطوم	٣×٩٠١٠	١٩٨١	٦٤ك	تجاري	٨
بنك النيل الازرق	الخرطوم	اي ٩٠٢٠	١٩٨١	١٢٨ ك	تجاري	٨
شركة الالبان	الخرطوم	اي ٩٠٤٠	١٩٨٣	٢٥٦ ك	تجاري	٨
البنك الاسلامي السوداني	الخرطوم	اي ٩٠٢٠	١٩٨٣	٢٥٦ ك	تجاري	٨
بنك الخرطوم	الخرطوم	١٤× اي٩٠١٠	١٩٨٣	٦٤ ك	تجاري	٨
بنك التضامن الاسلامي	الخرطوم	اي ٩٠٢٠	١٩٨٤	٢٥٦ ك	تجاري	=
و) النظم الحديثة (بليسي) البنك الاهلي	الخرطوم	بليسي ٢٣	١٩٨١	١٢٨ ك	تجاري	٨
البنك الاهلي	ام درمان	،، ،،	١٩٨٣	،،	،،	،،
البنك الاهلي	بورتسودان	،، ،،	١٩٨٣	،،	،،	،،
قسم الفيزياء جامعة الخرطوم	الخرطوم	،، ،،	١٩٨٤	،،	،،	
الجيش	الخرطوم	،، ،،	١٩٨٤	،،	تجاري وعملي	٨
الامدادات الطبية	الخرطوم	،، ،،	١٩٨٤	،،	تتجاري	
المجلس القومي للبحوث	الخرطوم	،، ،،	١٩٨٤	،،	علمي	

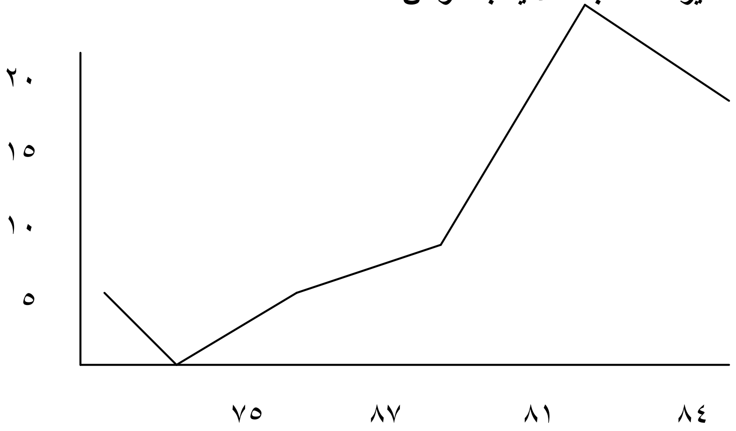
[2]

[2] مجلة الدراسات السودانية– العدد الاول – المجلد السابع أغسطس ١٩٨٩م

اسم المؤسسة	مكان التركيب	نوع الحاسب الالي	سنة التركيب	نوع التطبيقات
جامعة الخرطوم	قسم الفيزياء	كومادور	١٩٨٢	علمي
جامعة الخرطوم	الدراسات البيئية	شارب ب ب س ابل	١٩٨٢	علمي
جامعة الخرطوم	كلية الهندسة	ابل ١١	١٩٨٢	علمي
جامعة الخرطوم	العلوم الرياضية	بي بي سي	١٩٨٢	علمي
جامعة الخرطوم	الزراعة	ابل ١١	١٩٨٣	علمي
جامعة الخرطوم	مكتب المدير	الرايد ١٠٠	١٩٨٣	تجاري
جامعة الخرطوم	كلية الطب	وانق بي سي	١٩٨٤	علمي
الادارة القومية للطاقة	الخرطوم	هايبريون	١٩٨٣	علمي
موبيل اويل	الخرطوم	ابل ١١ اي بي ام	١٩٨٣	علمي
شل	الخرطوم	اي بي ام بي سي	١٩٨٣	تجاري
ادارة البترول	؟	؟	؟	؟
جامعة الجزيرة	ود مدني	ابل ١١	١٩٨٣	علمي
مشروع الطاقة الثالث	الخرطوم	ابل ١١	١٩٨٣	علمي

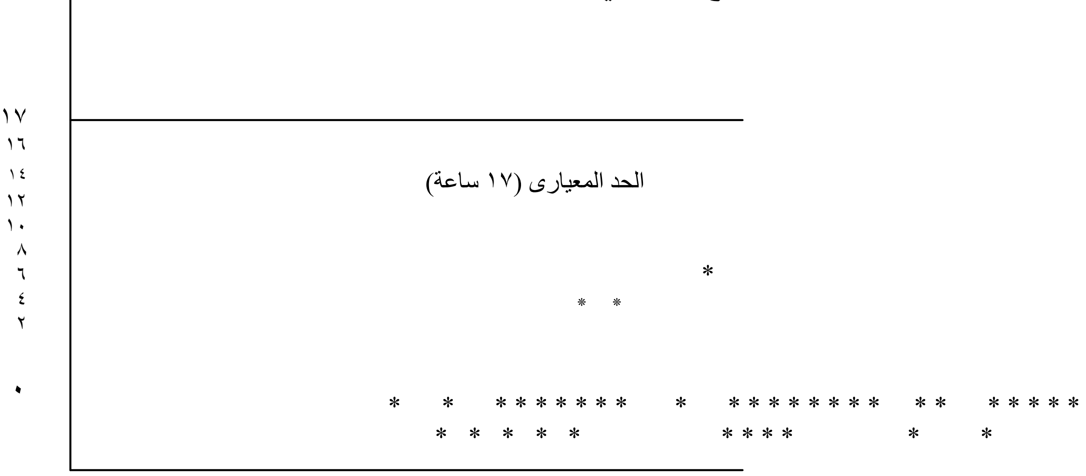
رسم رقم (١)

مسيرة الحاسبات الالية بالسودان



سنة التركيب

رسم رقم (٢)
الواقع التطبيقي للحاسبات الالية بالسودان



عدد ونوع الحاسبات التي سوقت للمؤسسات السودانية

الشركة	النوع	العدد
آي سي ال	١) ام اي ٢٩	٢
آي بي ام	١) سستم ٣٤	٢
وانق	١) ام في بي ٢٢٠٠	٣
	٢) في اس ١٠٠	١
ان سي أر	١) آي ٩٠٠٠	٢٥
بليسي	١) اي بي اس	٧

الخاتمة :-

نسال الله تعالى ان نكون قد وفقنا فيما رمينا اليه

ونسالكم الدعاء

احمد عبد الرحمن على شريف

Abomona77@yahoo.com

Abomona77@hotmail.com

00249123842491

00249922346688

الفهرس

الباب الثالث