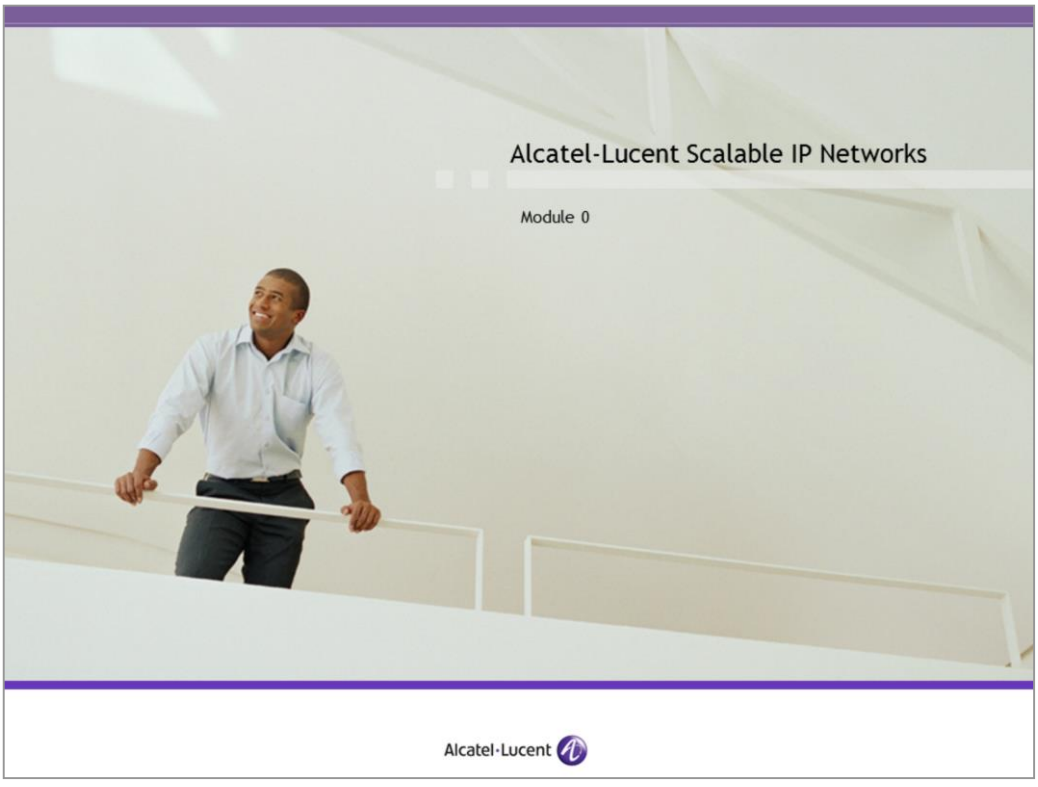
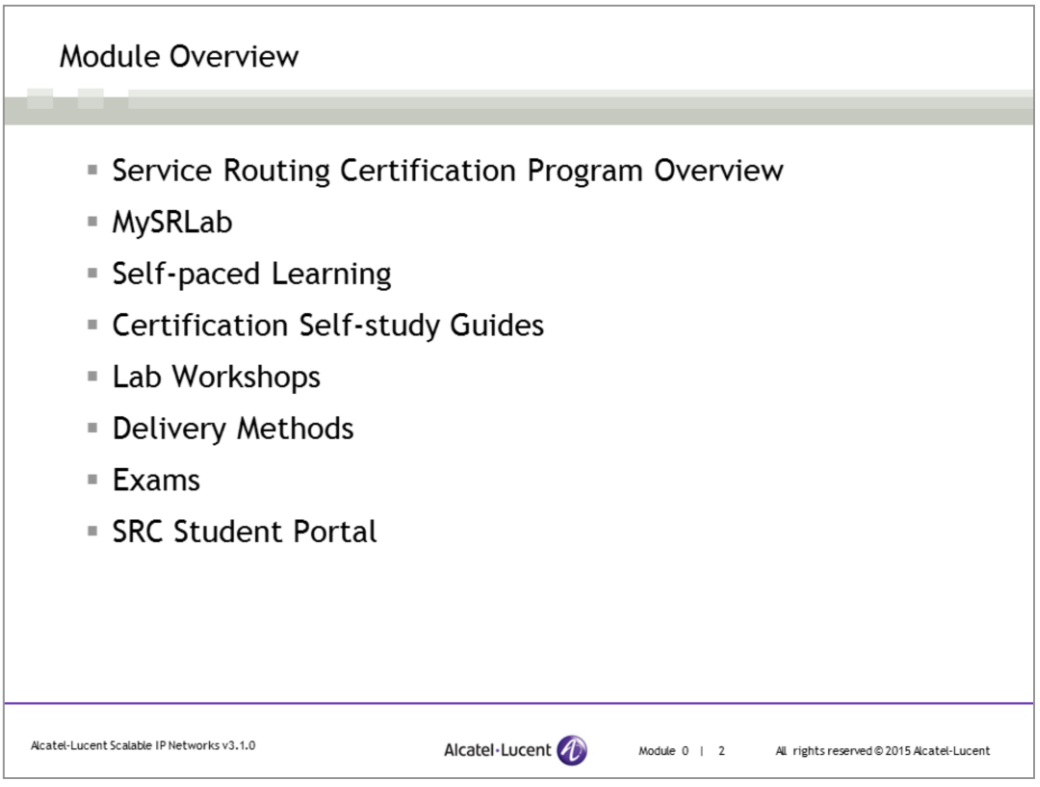


This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This course is part of the Alcatel-Lucent Service Routing Certification (SRC) Program. For more information on the SRC program, see www.alcatel-lucent.com/src

To locate additional information relating to the topics presented in this manual, refer to the following:

- Technical Practices for the specific products referenced in this course
- Internet Standards documentation such as protocol standards bodies, RFCs, and IETF drafts
- Technical support pages of the Alcatel-Lucent website located at: http://www.alcatel-lucent.com/support

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

The Alcatel-Lucent SRC Program – Five Certifications

ALCATEL-LUCENT
NETWORK ROUTING SPECIALIST I
4 DAYS / 1 COURSE / 1 WRITTEN EXAM

Alcatel·Lucent NRS I CERTIFICATION

ALCATEL-LUCENT
NETWORK ROUTING SPECIALIST II
18 DAYS / 4 COURSES / 4 WRITTEN EXAMS / 1 PRACTICAL LAB EXAM

Alcatel·Lucent NRS II CERTIFICATION

ALCATEL-LUCENT
TRIPLE PLAY ROUTING PROFESSIONAL
28 DAYS / 6 COURSES / 6 WRITTEN EXAMS / 1 PRACTICAL LAB EXAM

Alcatel·Lucent 3RP CERTIFICATION

ALCATEL-LUCENT
MOBILE ROUTING PROFESSIONAL
32 DAYS/ 7 COURSES / 7 WRITTEN EXAMS / 2 PRACTICAL LAB EXAMS

Alcatel·Lucent MRP CERTIFICATION

ALCATEL-LUCENT
SERVICE ROUTING ARCHITECT
46 DAYS / 10 COURSES / 10 WRITTEN EXAMS / 2 PRACTICAL LAB EXAMS

Alcatel·Lucent SRA CERTIFICATION

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

SRC Courses and Exams

Recommended courses	Alcatel-Lucent NRS I Certification	Alcatel-Lucent NRS II Certification	Alcatel-Lucent MRP Certification	Alcatel-Lucent 3RP Certification	Alcatel-Lucent SRA Certification
1. Alcatel-Lucent Scalable IP Networks	●	●	●	●	●
2. Alcatel-Lucent Interior Routing Protocols		●	●	●	●
3. Alcatel-Lucent Border Gateway Protocol					●
4. Alcatel-Lucent Multiprotocol Label Switching		●	●	●	●
5. Alcatel-Lucent Services Architecture		●	●	●	●
6. Alcatel-Lucent Virtual Private LAN Services					●
7. Alcatel-Lucent Virtual Private Routed Networks					●
8. Alcatel-Lucent Quality of Service			●	●	●
9. Alcatel-Lucent Multicast Protocols					●
10. Alcatel-Lucent Triple Play Services				●	
11. Alcatel-Lucent Advanced Troubleshooting					●
12. Alcatel-Lucent IP/MPLS Mobile Backhaul Transport			●		
13. Alcatel-Lucent Mobile Gateways for the LTE Evolved Packet			●		
Practical lab exams					
Alcatel-Lucent NRS II		●	●	●	●
Alcatel-Lucent MRP			●		
Alcatel-Lucent SRA					●

RECERTIFICATION - Certification is valid for three years.
You must complete additional exams to keep your certification active.

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 0 | 4
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

SRC Program Exam Profile

Exam Name	Exam Number	Exam Pre-requisites (4A0-XXX)
Alcatel-Lucent Scalable IP Networks	4A0-100	NA
Alcatel-Lucent Interior Routing Protocols	4A0-101	NA
Alcatel-Lucent Border Gateway Protocol	4A0-102	NA
Alcatel-Lucent Multiprotocol Label Switching	4A0-103	NA
Alcatel-Lucent Services Architecture	4A0-104	NA
Alcatel-Lucent Virtual Private LAN Services	4A0-105	NA
Alcatel-Lucent Virtual Private Routed Networks	4A0-106	NA
Alcatel-Lucent Quality of Service	4A0-107	NA
Alcatel-Lucent Multicast Protocols	4A0-108	NA
Alcatel-Lucent Triple Play Services	4A0-109	NA
Alcatel-Lucent Advanced Troubleshooting	4A0-110	NA
Alcatel-Lucent IP/MPLS Mobile Backhaul Transport	4A0-M01	NA
Alcatel-Lucent Mobile Gateways for the LTE Evolved Packet Core	4A0-M02	NA
Alcatel-Lucent Network Routing Specialist II Lab Exam	NRSII4A0	100, 101, 103, 104
Alcatel-Lucent Mobile Routing Professional Lab Exam	MRP4A0	100, 101, 103, 104, 107, M01, M02, NRSII4A0
Alcatel-Lucent Service Routing Architect Lab Exam	ASRA4A0	100, 101, 102, 103, 104, 105, 106, 107, 108, 110, NRSII4A0

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

MySRLab:
Like owning your own Service Router Lab

Do you need access to an SR lab to help you:

- Practice and build your service routing knowledge and configuration skills?
- Test new network and service features?
- Prepare for your NRS II, MRP and SRA exams?

The Alcatel-Lucent MySRLab service provides:

- Remote, private access (24x7) to an Alcatel-Lucent service router lab
- Multiple lab topologies for both wireline and mobility service environments
- Access to a suite of over 75 lab "practice" scenarios with optimal solutions
- Access to traffic simulation and analysis tools

Reserve your lab today at:

www.alcatel-lucent.com/src/mysrlab

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

SRC Self-Paced Learning Program

All of the resources you need to pass your SRC course and certification exams at your own pace

- NRS I and NRS II certification study guides (eBooks)
- Electronic copies of course material and lab guides
- MySRLab
- Other publications
- Special pricing on bundled self-paced learning packages

Find out how convenient learning can be:
www.alcatel-lucent.com/src/selfstudy

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Certification Self-Study Guides

- **Alcatel-Lucent Scalable IP Networks Self-Study Guide**

  ISBN: 978-0-470-42906-8

  Prepares the reader for the NRS I certification exam
- **Alcatel-Lucent Network Routing Specialist II Self-Study Guide**

  ISBN: 978-0-470-94772-2

  Prepares reader for the NRS II certification exams
- **Both guides include a CD with lab exercises and solutions**
- **Use MySRLab for hands-on lab exercises and exam preparation**

Alcatel-Lucent NRS II CERTIFICATION

Alcatel-Lucent NRS I CERTIFICATION

http://www.alcatel-lucent.com/srpublications

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

NRS II Lab Workshop: Learn from the Experts!

Overview

- Full-day lab workshop led by a service routing subject matter expert
- Students work independently through a series of assigned lab exercises
  - Two versions of the workshop (A & B) to register for-- ISIS focused workshop and an OSPF focused workshop
- Subject matter expert provides coaching/mentoring to students and reviews the proper solution to each exercise

Benefits

- Expert-level coaching
- Practice and build your SR configuration skills
- Ideal way to prepare for the NRS II lab exam

**** Classroom and virtual classroom delivery options available**

Register today at www.alcatel-lucent.com/src/coursereg

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Global Reach, Flexible Learning Options

Delivery Options

1. Classroom delivery from any of the Alcatel-Lucent locations below or at a local Alcatel-Lucent site
2. Virtual Classroom (live, instructor-led, online)
3. On-site delivery at your business location anywhere in the world

- **APAC**
  - Shanghai, China
  - Sydney, Australia
  - Melbourne, Australia
  - Wellington, New Zealand
  - Bangalore, India
  - Chennai, India
  - Gurgaon, India
  - Mumbai, India
- **Europe**
  - Antwerp, Belgium
  - Newport, UK
  - Paris, France
  - Cairo, Egypt
  - Istanbul, Turkey
- **N. America**
  - Plano, USA
  - Ottawa, Canada
- **CALA (via SRC certified training partner, INDC)**
  - Buenos Aires, Argentina
  - São Paulo, Brazil
  - Santiago, Chile
  - Bogota, Colombia
  - San Jose, Costa Rica
  - Mexico City, Mexico
  - Lima, Peru

Class schedules and registration are available at:
http://www.alcatel-lucent.com/src/coursereg

INDC (CALA) class schedules are available at:
www.indc.co.cr/courses/alu

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Exam Delivery

Written Exams

- Delivered by Prometric, a global provider of testing services
- 5000+ test sites worldwide
- **Register at:** www.prometric.com/alcatel-lucent

Lab Exams

- Administered at Alcatel-Lucent locations
- NRS II Certification
  - Half-day lab exam
- MRP Certification
  - Half-day lab exam
- SRA Certification
  - Full-day lab exam

Register at www.alcatel-lucent.com/src/examreg

PROMETRIC™

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

NRS II Composite Exam

New written exam for the NRS II certification track

Combines 3 exams into a single, integrated exam

- Alcatel-Lucent Interior Routing Protocols (4A0-101)
- Alcatel-Lucent Multiprotocol Label Switching (4A0-103)
- Alcatel-Lucent Services Architecture (4A0-104)

Exam questions: 100

Exam duration: 3.5 hours

Existing NRS II exams will continue to be available

- Students will have the option to take the individual written exams or the new composite exam

For re-certification purposes, the composite exam will replace the Services Architecture (4A0-104) exam

Register at www.alcatel-lucent.com/src/exams

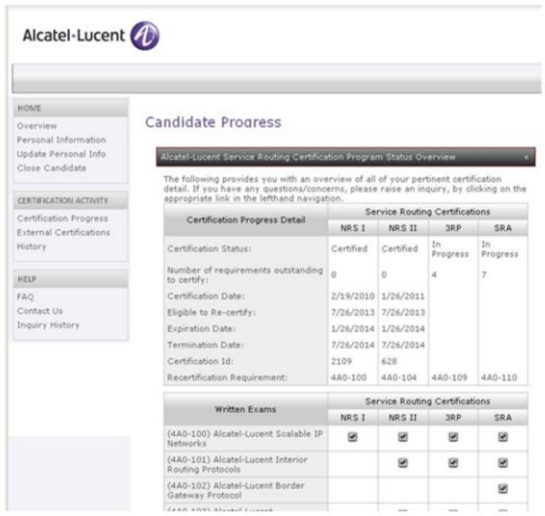
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

SRC Student Portal

Login to the SRC Student Portal to:

- Check your exam history
- Verify your certification status and reminder dates such as renewal, and expiry
- Download and display logos for your active certifications
- Publish your certification status to third parties
- Check on the status of your fulfillment items such as plaques, and diplomas
- Get program updates
- Review FAQs and get support



http://www.alcatel.lucent.com/src/studentportal

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Credit for Other IP Certifications

Are you Cisco or Juniper certified?

- You can receive exemptions from some of the SRC exams if you hold any one of the Cisco or Juniper certifications identified
- Certifications must be valid to receive exemptions
- Submit your request for exemptions at: http://www.alcatel-lucent.com/src/exemptions

Cisco Certifications	SRC Exam Exemption
Cisco Certified Network Associate (CCNA)	None
Cisco Certified Network Professional (CCNP)	None
Cisco Certified Network Professional (CCNP - Service Provider)	4A0-100
Cisco Certified Internetwork Professional (CCIP)	4A0-100
Cisco Certified Internetwork Expert (CCIE - Routing & Switching)	4A0-100/4A0-101/4A0-102
Cisco Certified Internetwork Expert (CCIE - Service Provider)	4A0-100/4A0-101/4A0-102
Juniper Certifications – M- Series	
Juniper Networks Certified Internet Associate M-Series (JNCIA-JUNOS)	None
Juniper Networks Certified Internet Specialist (JNCIS-SP)	4A0-100
Juniper Networks Certified Internet Professional (JNCIP-SP)	4A0-100
Juniper Networks Certified Internet Expert (JNCIE-SP)	4A0-100/4A0-101/4A0-102
Juniper Certifications – E- Series	
Juniper Networks Certified Internet Associate (JNCIA-E)	None
Juniper Networks Certified Internet Specialist (JNCIS-E)	None
Juniper Networks Certified Internet Professional (JNCIP-E)	4A0-100
Juniper Certifications - J - Series	**None**

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 0 | 14 All rights reserved © 2015 Alcatel-Lucent

Course Objectives

Upon successful completion of this course, you should be able to:

- Describe the use of the Alcatel-Lucent Service Router family products
- Execute basic CLI commands of the Alcatel-Lucent 7750 SR
- Describe the purpose and operation of common Layer 2 technologies
- Develop an IP address plan using IP subnetting and address summarization
- Explain the difference between static routing and dynamic routing protocols
- Describe how MPLS tunnels are used to support VPN services
- Describe the VPN services supported on the Alcatel-Lucent 7750 SR

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Course Timeline

Day 1

- Module 0 — Course Introduction
- Module 1 — Internet Overview
- Module 2 — Service Router Components and CLI
  - Lab 1 — Lab Infrastructure Configuration and Verification
- Module 3 — Data Link Overview

Day 2

- Module 3 — Data Link Overview
- Module 4 — Layer 3 and IP Services
  - Lab 2.1 — IP Address Plan Design
  - Lab 2.2 — Router Interface Configuration

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Course Timeline (cont'd)

Day 3

- Module 4 — Layer 3 and IP Services
  - Lab 2.3 — ICMP and ARP Operation
- Module 5 — IP Routing Protocol Basics
  - Lab 3 — Static Routing
  - Lab 4 — OSPF
  - Lab 5 — BGP (instructor's demo)

Day 4

- Module 5 — IP Routing Protocol Basics
  - Lab 6 — IP Filters
- Module 6 — Services Overview
  - Lab 7 — Services (instructor's demo)

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Course Prerequisites and Follow-On

Suggested prerequisites

- There is no prerequisite for this course, however, familiarity with binary arithmetic is an asset

Alcatel-Lucent Scalable IP Networks Exam

- To ensure full comprehension of the material covered in this course, it is recommended that student take this exam

Suggested follow-on courses

- Based on the material covered in this course, it is recommended that, upon successful completion of the Scalable IP Networks course, the student enroll in the Alcatel-Lucent Interior Routing Protocols course

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 0 | 18 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Administration

- Registration
- Facility information
- Restrooms
- Communications
- Materials
- Schedule
- Introductions
  - Name and company
  - Experience
- Questions

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

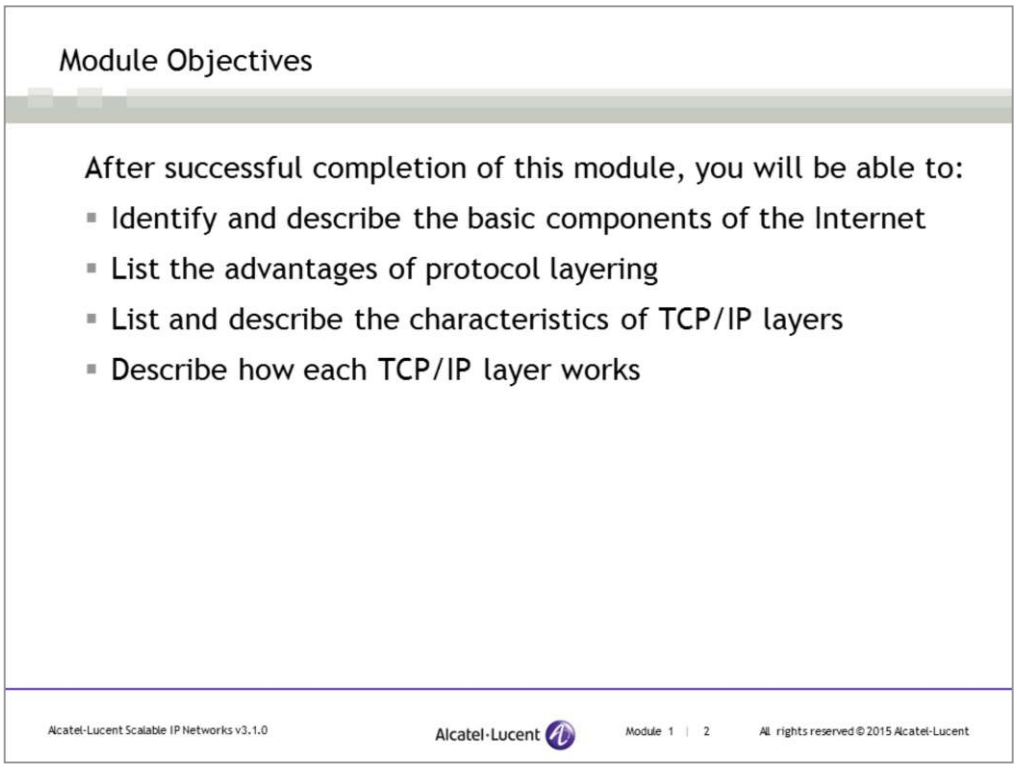
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Alcatel-Lucent Scalable IP Networks (ASIN)

This course is part of the Alcatel-Lucent Service Routing Certification (SRC) Program. For more information on the SRC Program, refer to the Alcatel-Lucent website at www.alcatel-lucent.com/src.

To locate additional information relating to the topics presented in this manual, refer to the following:

- Technical practices for the specific product
- Internet standards documentation such as protocol standards bodies, RFCs and IETF drafts
- Technical support pages of the Alcatel-Lucent website located at www.alcatel-lucent.com/support

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

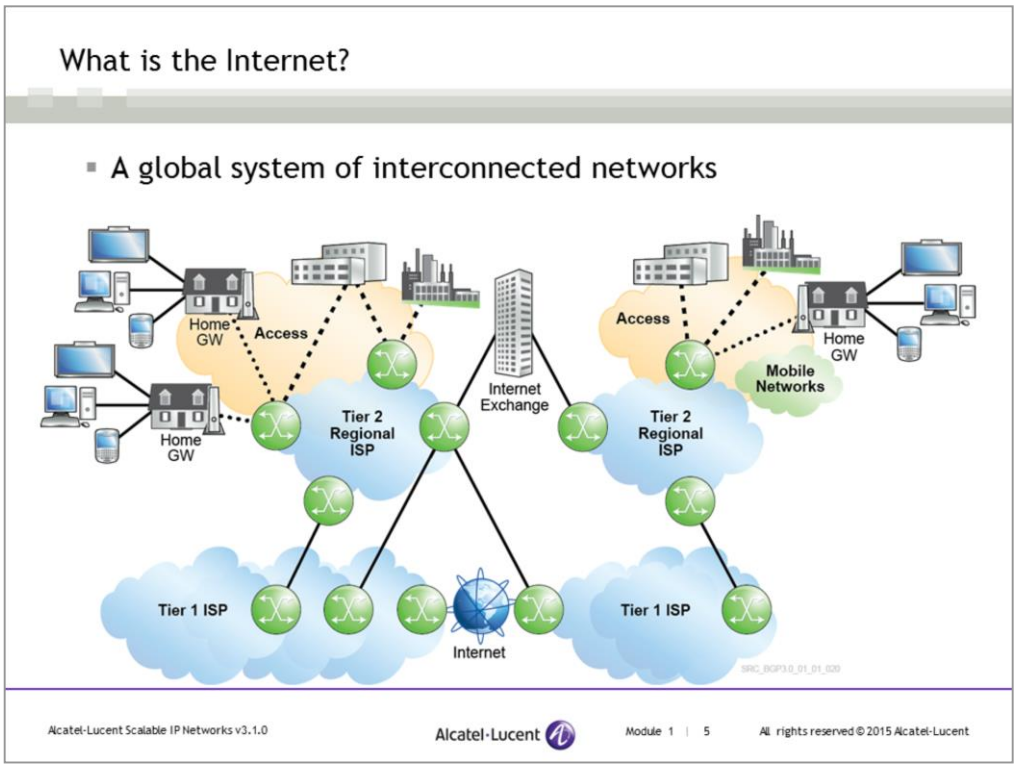
After the successful completion of this section, you will be able to:

- Define Internet
- Describe the roles and functions of the content provider and the service provider
- Describe the functions of service provider tiers
- Describe the functions of internet exchange points and point of presence
- Identify the Internet connection components required between home users and local ISPs

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 1 | 4
All rights reserved © 2015 Alcatel-Lucent

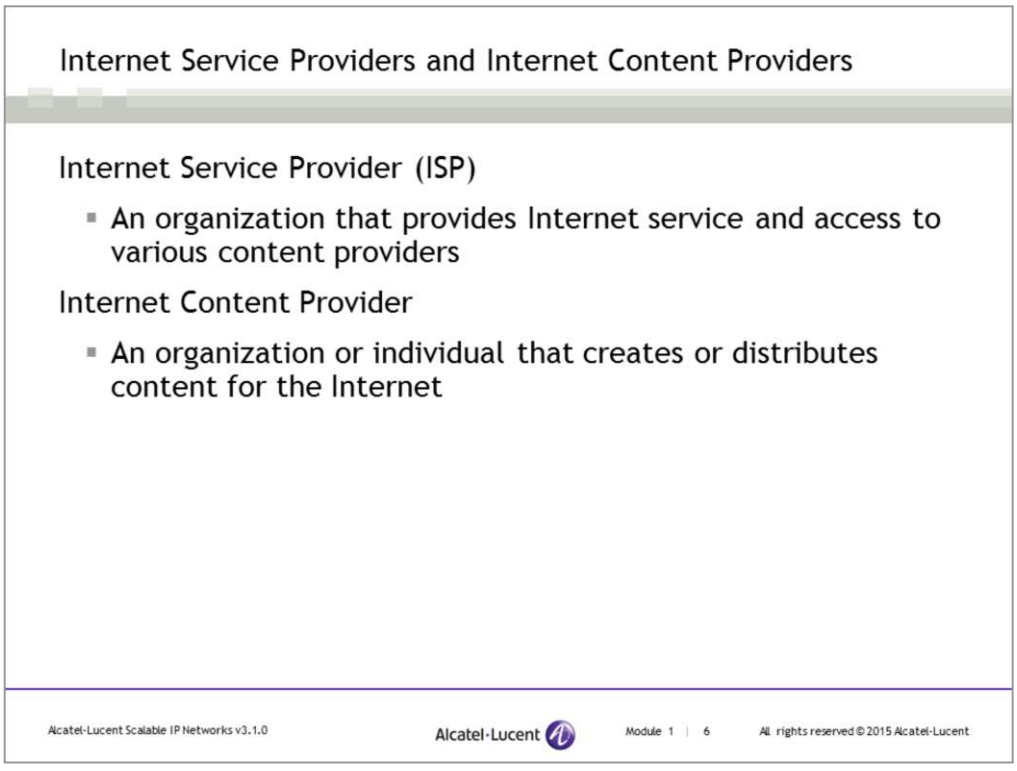
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Internet is a global system of networks that relies heavily on the interconnections provided by Internet service providers (ISPs), content providers and regional Internet exchange points. The Internet can also be described as a continuous, interconnected set of all of the public IP (v4 or v6) networks, advertised and shared across the globe. It is an inter-connected network of networks that allows every ISP to reach every other ISP in the world.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



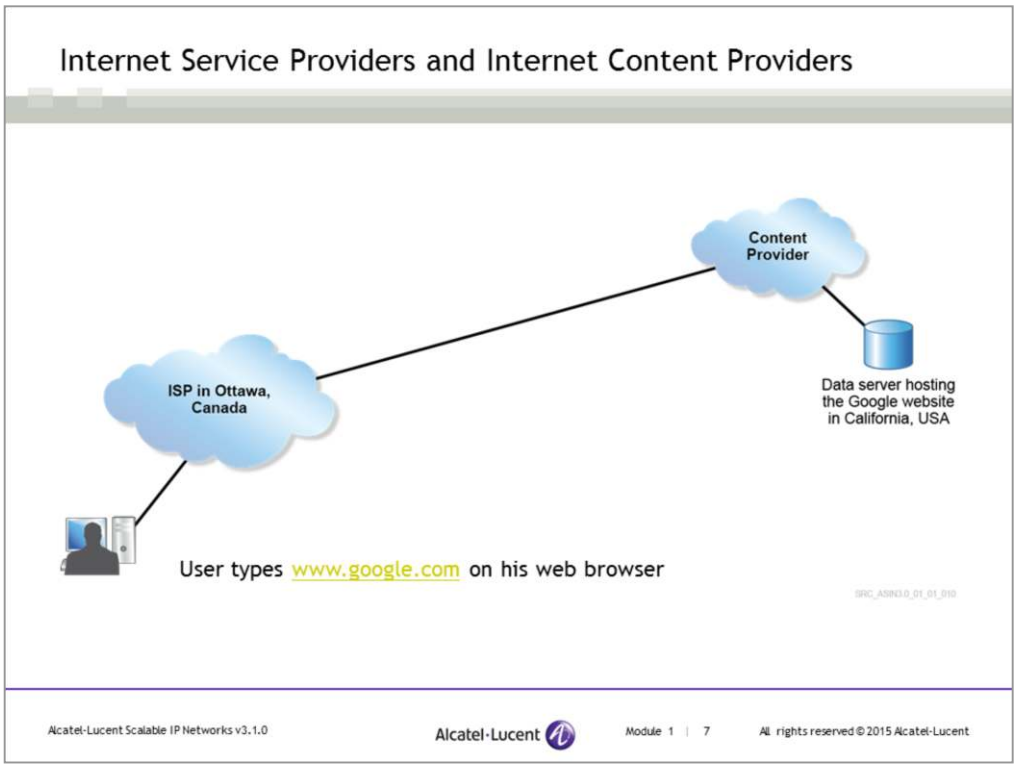
The terms *content provider* and *service provider* can be applied to a broader scope other than the Internet. Note that for the purposes of this course, *content provider* and *service provider* are referred to only in the context of the Internet.

Internet Service Provider vs Internet Content Provider

- Anyone that offers Internet connectivity can claim to be an Internet provider or service provider. The term **Internet service provider** covers everything from a provider with a multimillion-dollar backbone and infrastructure to a provider with one router and an access server in their garage.
- An **Internet content provider** creates or distributes the online content. This information typically resides on data servers. Access to these data servers occurs by using application protocols, a concept that will be discussed later.
- The most common example of an **application protocol** that is used to access information is Hypertext Transfer Protocol (HTTP), which is the fundamental protocol of the world wide web (WWW).
- By using HTTP, users can access information from any server that contains the particular information (the website).
- For example, using HTTP protocol, users can simply type `www.google.com` into their web browser and obtain information from the website or the data server that hosts www.google.com.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



It is quite typical for an Internet user to obtain content from servers outside of their vicinity. The Internet gives any user access to content on servers located anywhere in the world.

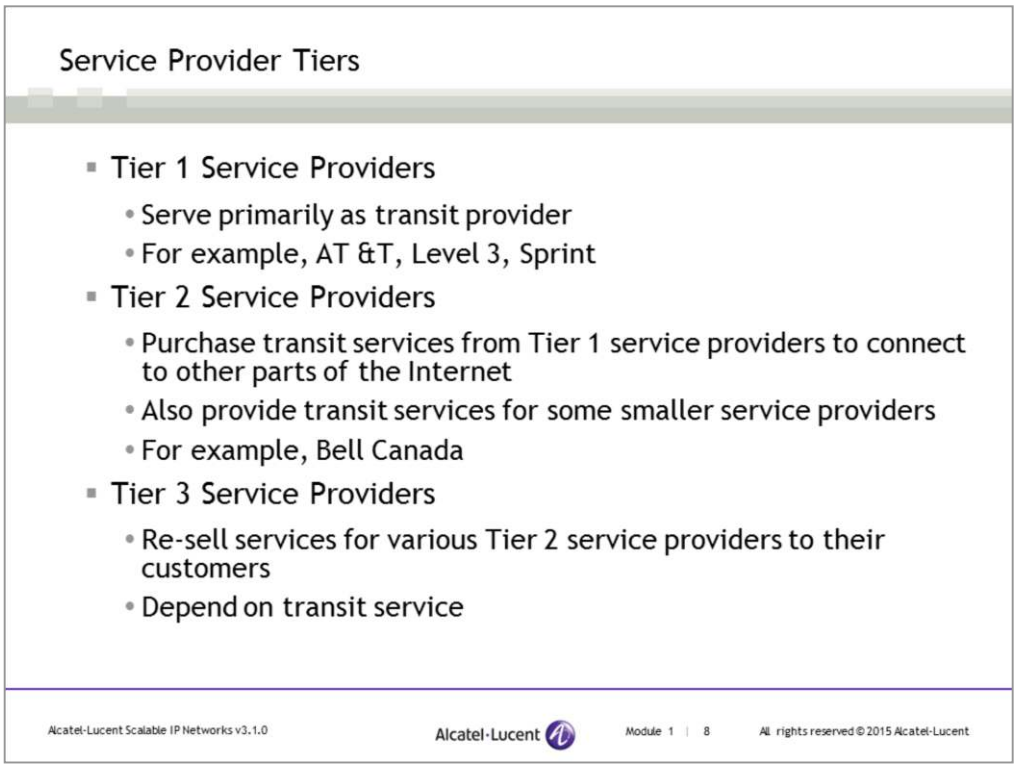
Considering the previous example of our user in Ottawa accessing content in California, the user in Ottawa, Canada types `www.google.com` into his web browser and obtains information from the data server hosting Google. The user in Ottawa obtains services from a local ISP. The data server hosting Google is in California, connected to its content provider. The ISP in Ottawa and the content provider in California must be able to connect directly to each other, OR must be able to use the service of another ISP that provides transit services to the ISP in Ottawa and the content provider. Only then will the local user send and receive traffic from the Google server.

This slide displays the configuration described above.

Apart from web access, ISPs can also provide e-mail access with multiple e-mail accounts, data storage, and broadcast television services.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Tier 1 Service Providers

- In this content of Tier 1, the service provider and the network are interchangeable.
- A Tier 1 network does not purchase transit-by-transit service from any other network to reach any other portion of the Internet.
- To be a Tier 1 network, a network must peer with every other Tier 1 network.
- A new network cannot become a Tier 1 network without the explicit approval of every other Tier 1 network, because any network's refusal to peer prevents the new network from being considered a Tier 1 network.

Tier 2 Service Providers

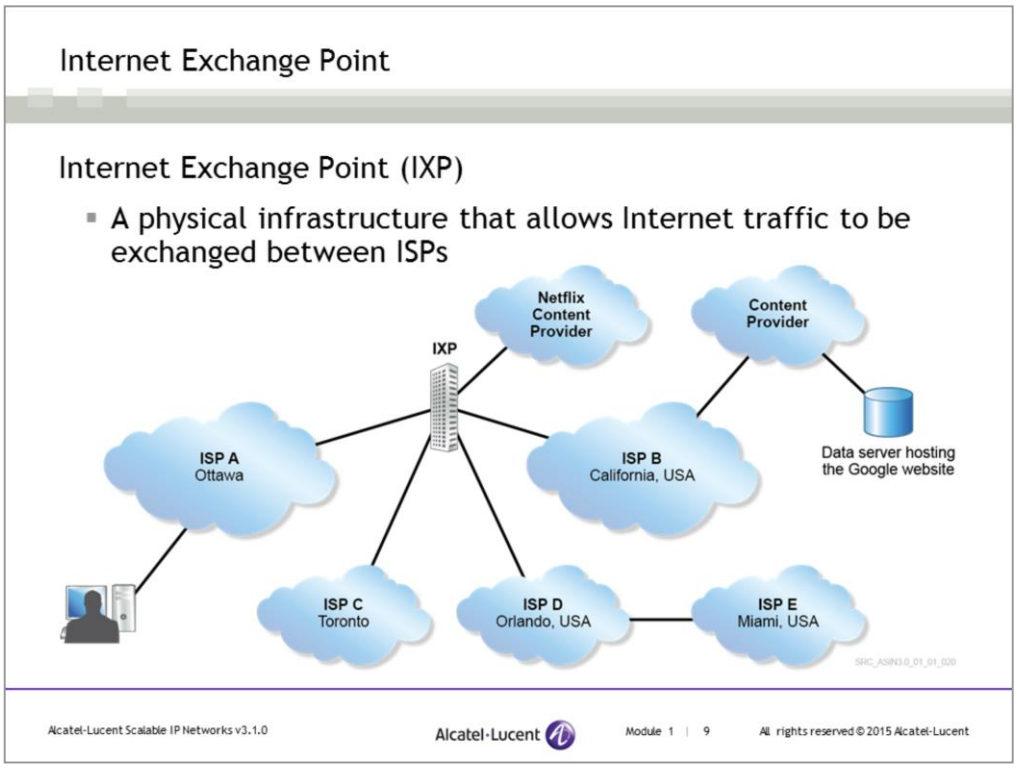
- Tier 2 service providers purchase transit services from one or more Tier 1 service providers.

Tier 3 Service Providers

- Tier 3 service providers are smaller than Tier 2 service providers. Tier 3 service providers require a Tier 1 or Tier 2 service provider for transiting to parts of the Internet.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Internet Exchange Point (IXP)

- IXPs provide interconnections between Internet service providers. IXPs enable the exchange of information among each ISP's customer through information exchange at local points, which negates the need to traverse or backhaul traffic through major points to reach the Internet. Think of IXPs as serving the same purpose as a centralized train station or an airline hub. Packets arrive from various ISPs and are pushed to the next ISP for delivery to their ultimate destination through Internet routing protocols.

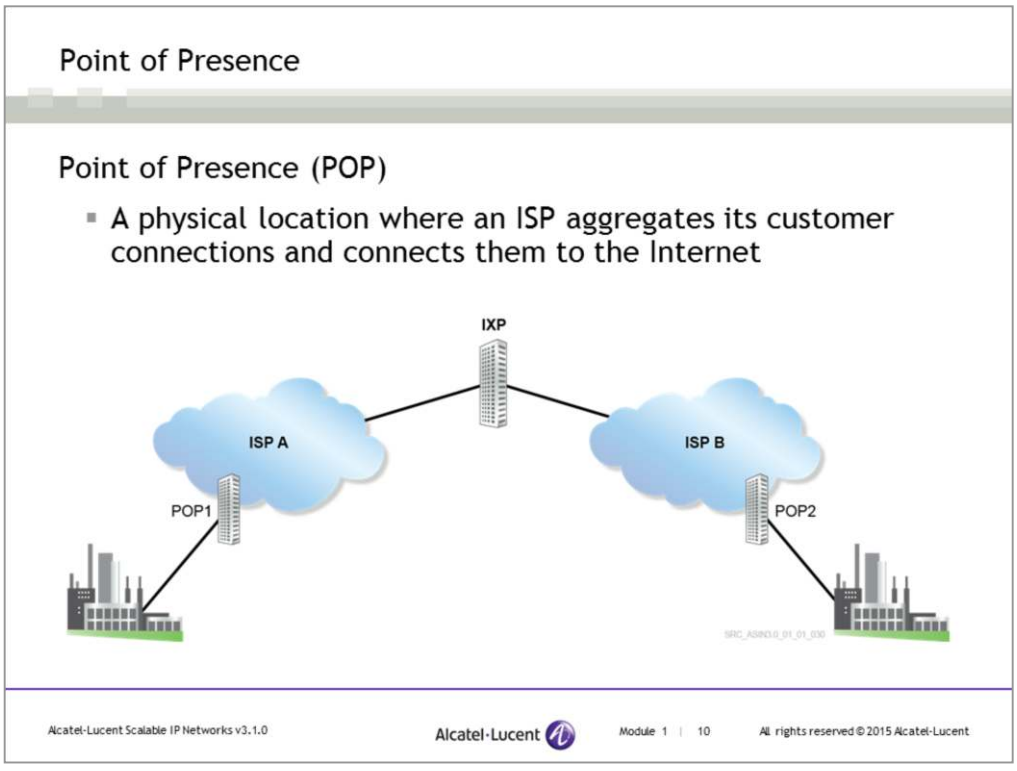
- It is quite typical for an Internet user to obtain content from servers outside of their vicinity. The Internet gives any user access to content on servers located anywhere in the world.

- For example, our user is in Ottawa, Canada, obtaining services from a local ISP (ISP A). The data server hosting Google is in California, connected to its content provider. ISP A and the content provider must be able to connect directly or indirectly through the service of another ISP that provides transit services to both ISP A and the content provider. Only then will the local user send and receive traffic from the Google server. Since the data server can be accessed through an ISP in California (ISP B), ISP A and the content provider can connect indirectly through ISP B using an IXP.

- In this slide, ISP A in Ottawa has a single physical connection to an IXP and can exchange traffic with any ISPs connected to the IXP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

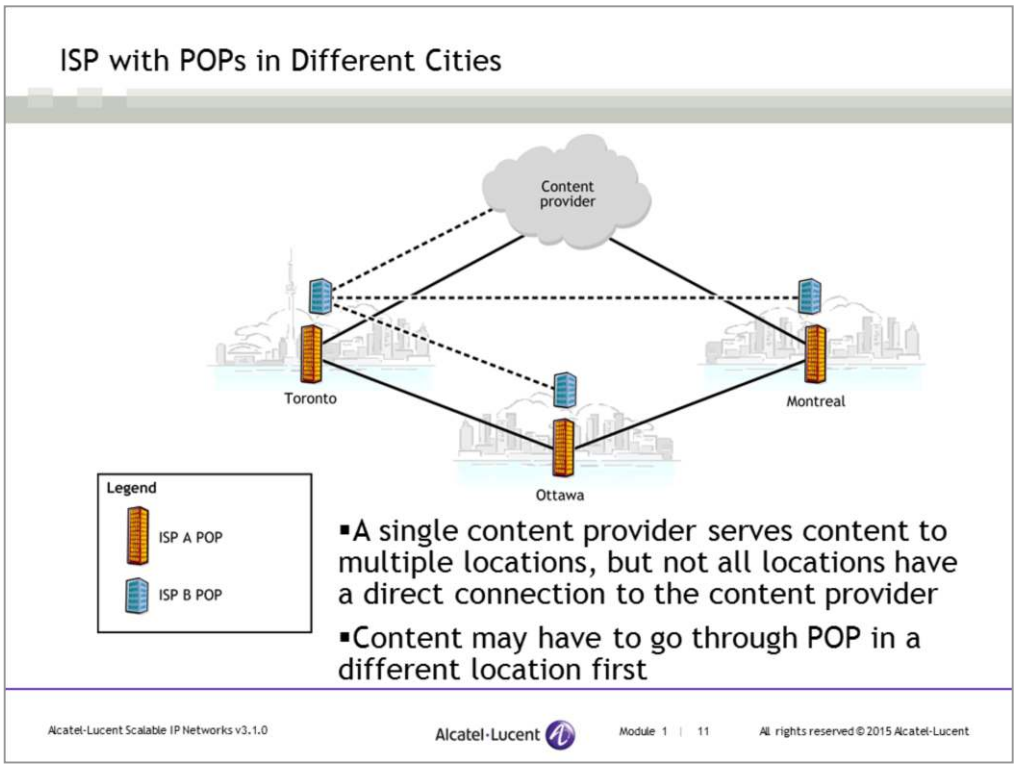


Point of Presence (POP)

- POP is an infrastructure that allows users to connect to the Internet.
- In this example, user A requires Internet service from its service provider, ISP A, by connecting to access or hosting facilities in that provider's POP, POP1. Similarly, user B also requires Internet service from its service provider, ISP B, by connecting to that provider's POP, POP2.
- Interconnections between service providers, ISP A and ISP B, are facilitated through an exchange point, IXP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Today's Internet backbone is quite complex. The backbone is a collection of service providers with connection points over multiple regions. These connection points are called points of presence (POPs). The collection of POPs and the interconnections between them form the provider networks.

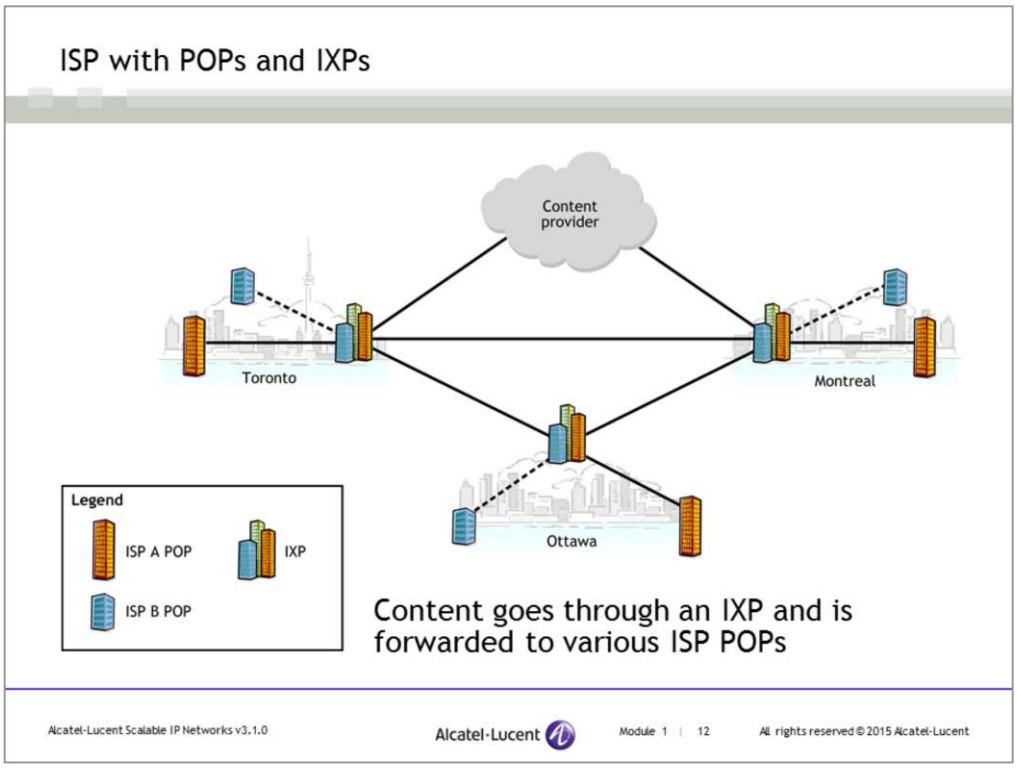
Customers who purchase Internet service from these service providers are connected through access or hosting facilities located in the service provider's POP. Service providers may have direct or indirect access to content providers. Customers are the end hosts that receive Internet service from their service provider.

In this slide, a single content provider serves content to multiple locations through POPs. ISP B in Montreal is not connected directly to the content provider. If ISP B wants to reach the content provider, it must send its traffic to Toronto first (which is directly connected to the content provider). Similarly, ISP A's POP in Ottawa must send its traffic through Toronto or Montreal to reach the content provider.

Service providers with POPs throughout the country are commonly referred to as national providers. Service providers that cover specific regions are referred to as regional providers. To enable customers of one provider to reach customers connected to another provider, traffic is exchanged at public IXPs or through direct interconnections. The term ISP is commonly used to refer to any entity that provides Internet connectivity service directly to the end user or to other service providers.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



As previously mentioned, interconnections between providers are facilitated through exchange points known as IXPs. Because IXPs serve as the switching points for a large amount of traffic, it is critical that they switch packets from one provider network to another as quickly and reliably as possible.

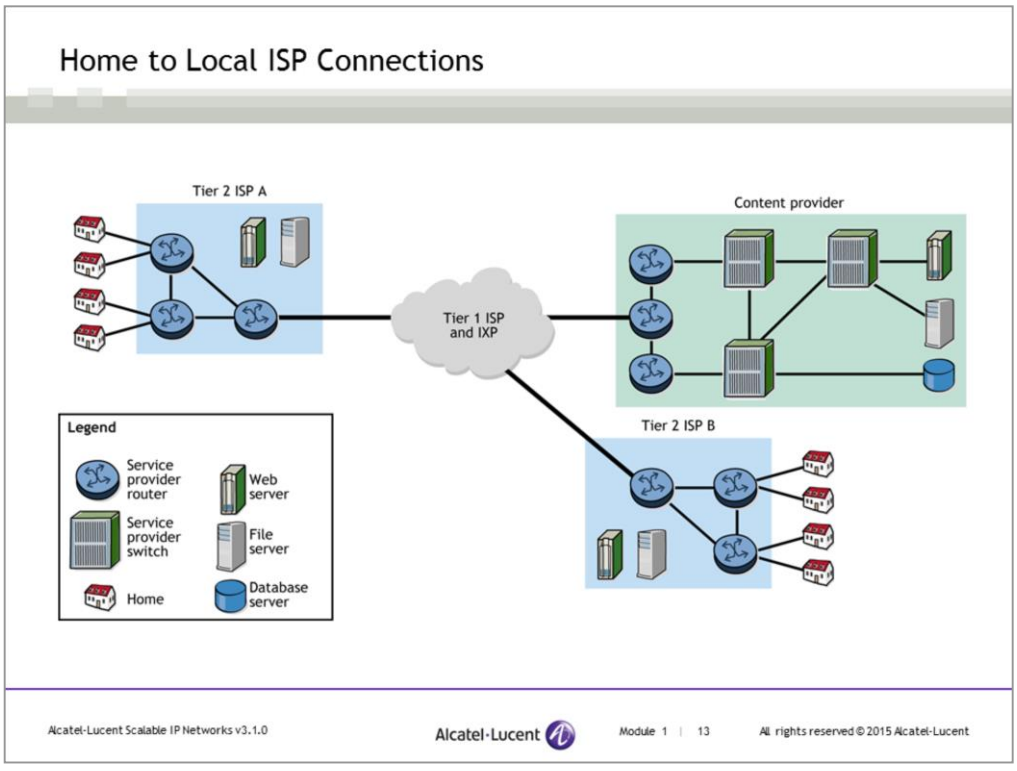
With an IXP at the city level, traffic between various ISPs and content providers can be handled within the same city. If a content provider is connected to the IXP in a local city, the traffic between the ISP POPs in that city and the content provider is localized.

In this slide, ISP A's POP and ISP B's POP in Toronto can communicate with each other locally through the IXP in Toronto.

Without the local IXP, the traffic between ISPs may need to be carried to another city with an IXP before the traffic arrives at the destination ISP. For example, if there were no local IXPs in Toronto, a user using ISP A in Toronto wanting to access a service at his office in Montreal would have his traffic routed via Ottawa's IXP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



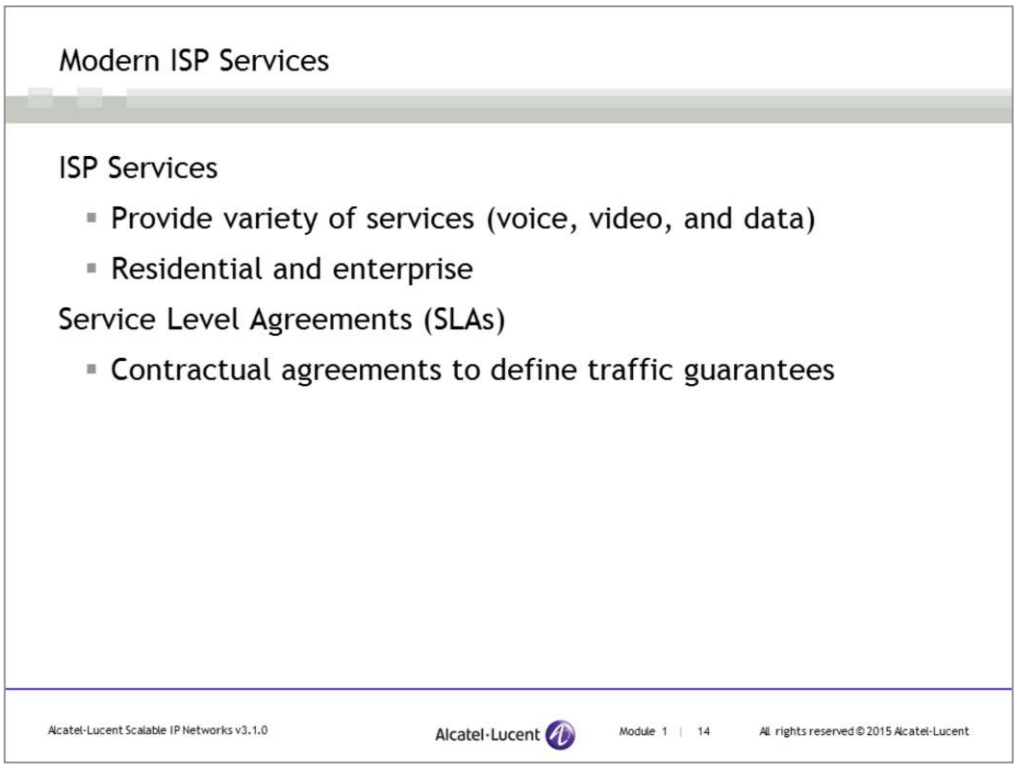
The slide shows a typical scenario where home users are connected to the Internet.

Home users connect to a local service provider, which can be a Tier 2 or Tier 3 service provider, depending on the size of their local ISP.

For example, two home users may want to perform video messaging with each other. In this scenario they are connected to two independent ISPs. One home user is connected to a Tier 2 service provider, ISP A, while the other home user is connected to a different Tier 2 service provider, ISP B. ISP A is connected to ISP B through an IXP or through a Tier 1 ISP that agreed to forward their traffic. The Tier 1 ISP may also connect directly with a content provider or through a Tier 2 ISP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



ISP Services

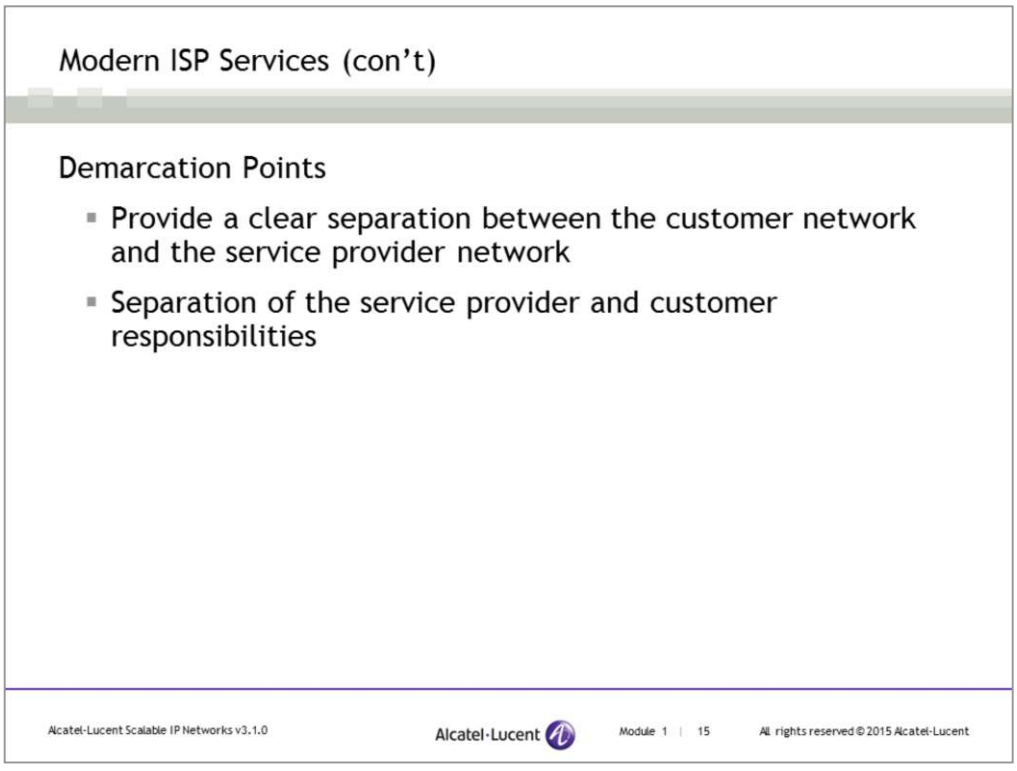
- Traditionally, ISPs provided access to basic services such as email and web surfing through a modem dial-up. The connections were low speed with the theoretical limit of 56 Kbps at the peak of modem technology.
- Nowadays, along with Internet access, modern ISPs can also be content providers or can peer with several content providers to provide their users with a variety of services, mainly voice, video, and data applications. To compete with traditional cable, satellite and Telecom providers, modern ISPs bundle the major services (voice, video and data) into what is referred to as a *triple play package*. In contrast, some cable and satellite providers now offer Internet services to compete with Telecom providers and other ISPs.
- Cost reduction is one major motivation for bundling services that were traditionally offered as individual services. Another motivation is to offer customized services with varying price points. For example, an ISP may offer end users three packages - a basic service, a premium service, and an elite service. The package with higher service utilization costs more than the package that offers a basic service. The basic package may offer a 10 Mbps combined voice, Internet, and basic video service; the premium package may offer 20 Mbps combined voice and Internet service, but basic video service; and the elite package may offer 40 Mbps voice, high-speed Internet, and high definition video services.

Service Level Agreements

- A service level agreement is a contractual agreement between an ISP and its customers that defines traffic flow guarantees. It may include penalties when traffic is not delivered in compliance with the service level agreement.
- In addition to residential customer traffic needs, ISPs typically provide business traffic needs for enterprises. A medium-to-large enterprise that requires the ISP's geographical presence to connect to its offices or to other enterprise organizations will have traffic requirements for bandwidth and timely delivery that are well beyond that of the home user. The enterprise may require additional services from an ISP such as web hosting, and services for inter-site connectivity. Typically, the traffic that travels through the ISP's network is critical to the daily operations of the enterprise. The delivery of this type of traffic is usually guaranteed by the ISP with a service level agreement.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

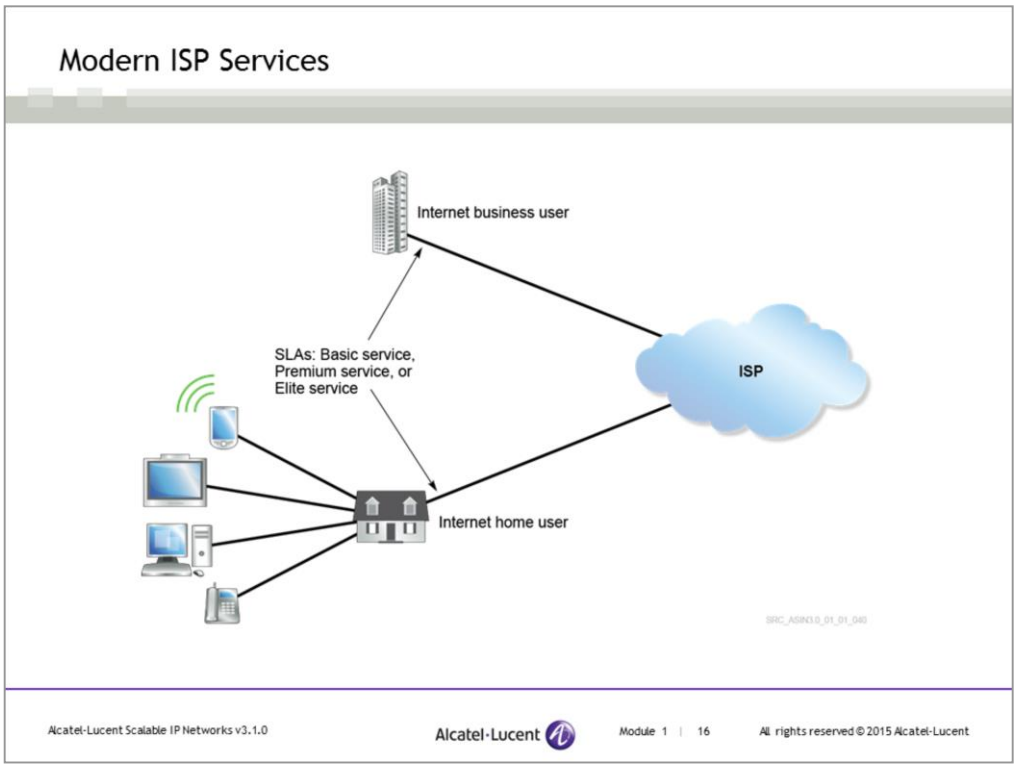


Demarcation Points

Demarcation points provide separation between the service provider and the customer. The demarcation point is where the service provider's responsibility ends and the customer's responsibility begins.

All rights reserved © 2015 Alcatel-Lucent

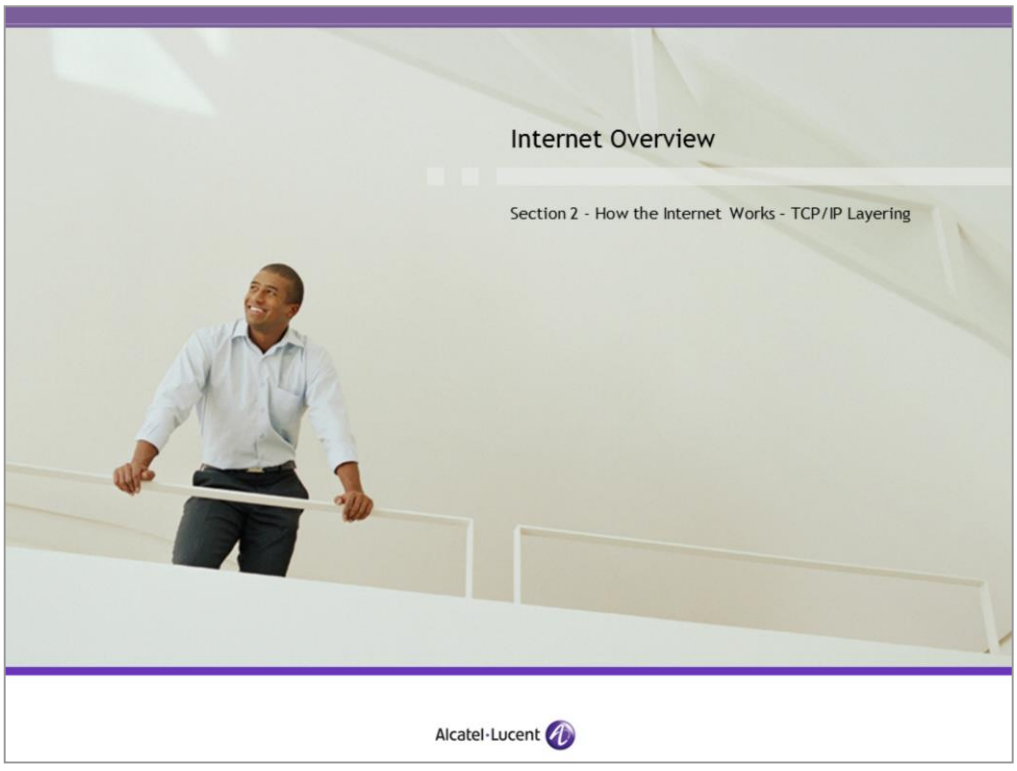
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows that Internet users (businesses, consumers, etc.) can access a variety of services. These services can be phone service, mobile service, broadcast TV service, and Internet service from an ISP. When a user obtains service from an ISP, there is a contractual agreement, or SLA, that defines the level of service. Basically, the more the user pays for the service, the higher is the level of service provided by the ISP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

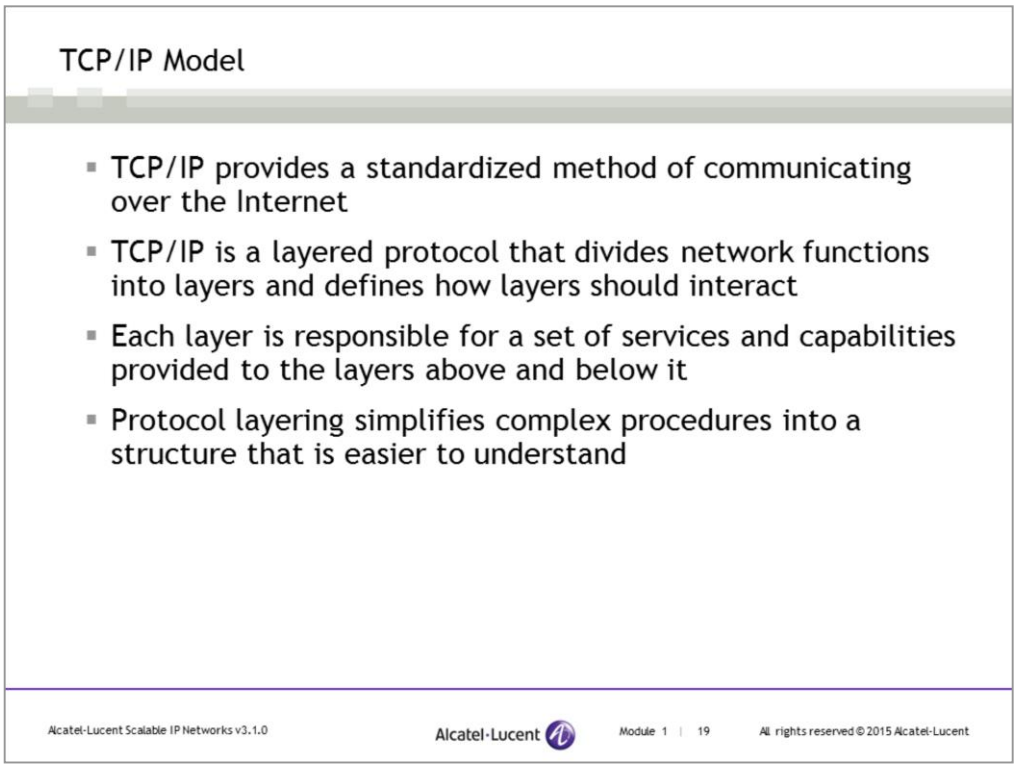
After the successful completion of this section, you will be able to:

- Explain the benefits of protocol layering
- Describe the relationship between TCP/IP and OSI
- Describe the characteristics of the four TCP/IP layers
- Describe the encapsulation of each of the four TCP/IP layers

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The TCP/IP model is designed to allow all components of the network to work together, regardless of which vendors the parts are brought from. To make the network components work together, TCP/IP divides network functions into layers and defines how those layers should interact.

Layering information can be compared with regular postal service, where there are several distinct functions:

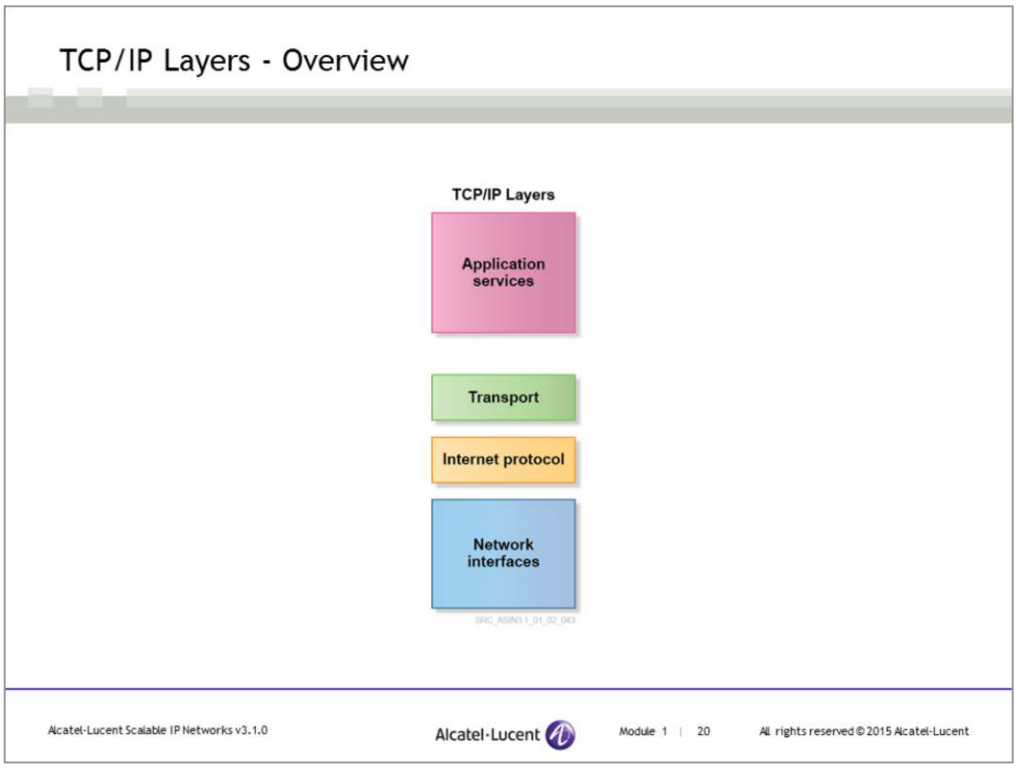
- Creating the letter
- Placing the letter in an envelope and writing the sender's and recipient's addresses
- Choosing the type of delivery for the letter (same-day service, registered mail, etc.)
- Placing the appropriate stamp on the letter to pay for the service
- Physically sending the letter via carriers; for example, by truck or airplane

After the sender writes the letter, all functions listed above are relevant to transporting the letter to the appropriate destination. At the destination, the letter is received by the recipient, and depending upon the transport service, an acknowledgement may be sent to the sender confirming the receipt of the letter. The letter can then be removed from the envelope and its contents read.

The layering of TCP/IP information is treated in a similar fashion. Information transmitted across the Internet is broken down into pieces, called *packets*. The objective is to reliably send packets to a destination with a given IP address through different networks. Each TCP/IP layer adds the pertinent information (destination, error checks, etc.) at the beginning of the data, thereby adding more information to the data. As the data is sent from the sender to the receiver, the data passes through several other systems. These systems only check the relevant header information for the layers that they are interested in. The systems use this information to pass the data to the appropriate destination.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The network protocol suite defines the protocols and technologies that support the interconnection of a diverse array of hardware and systems to support the operation of a wide range of applications over the network. Anyone who has used an Internet application, such as a web browser or email, can appreciate the complexity of the systems that are required to support these applications.

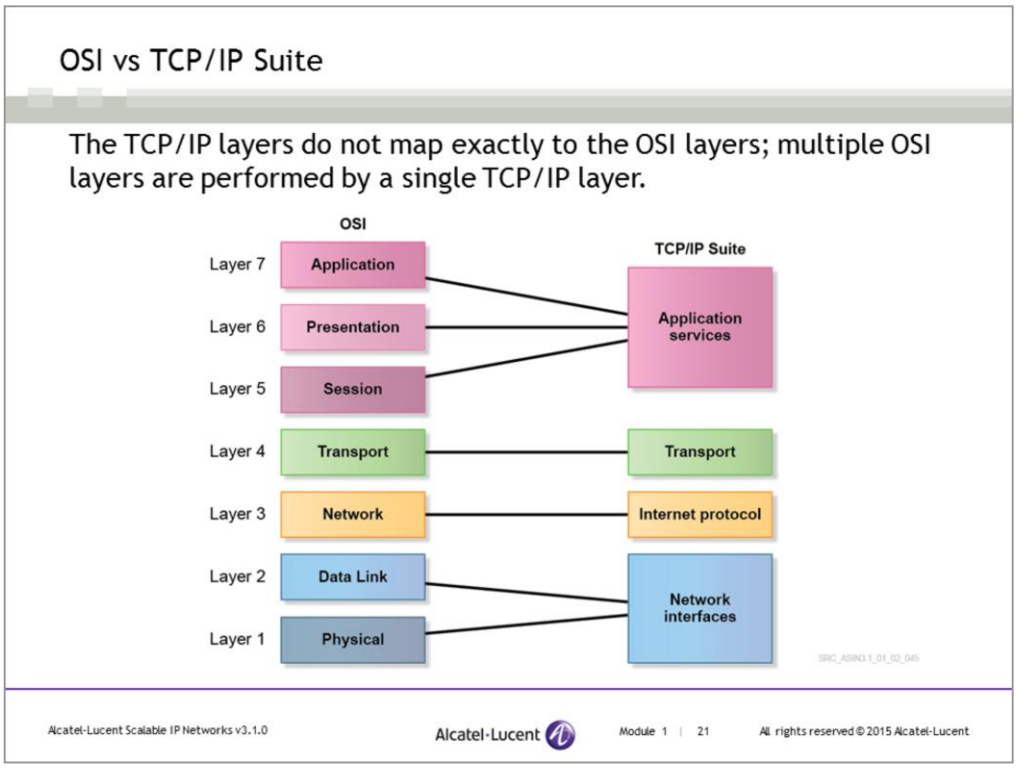
The layering of protocols simplifies this complex problem by dividing the protocol into a number of smaller functions. Each layer performs a specific function that contributes to the overall functioning of the network. System participating in the protocols may not need to participate at every level, making it easier to move from one point on the Internet to another with minimal effort. For example, network devices on the Internet may know only the destination address of information but need not know that the information in the packet is email or Web traffic.

The TCP/IP protocol suite, also known as the Internet protocol suite, contains four layers of technology.

- The application services layer provides all of the services that are available to users of the Internet.
- The two intermediate layers (transport and Internet protocol) provide a common set of services that are available to all of the Internet applications and operate on the Internet hardware infrastructure.
- The network interfaces layer includes all of the hardware that comprises the physical infrastructure of the Internet.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The TCP/IP suite differs from the OSI model in that the TCP/IP suite uses four protocol layers and the OSI model uses seven layers. The slide shows the protocol layer relationship between the two models.

Network interfaces — This layer defines the actual interface between network nodes and contains the functionality of both the physical and data link layers of the OSI model. Protocols such as Ethernet describe both the framing of data (Layer 2) and the physical transmission of the frame over the media (Layer 1). This layer is often referred to as Layer 2 because it provides OSI Layer 2-type services to the IP layer.

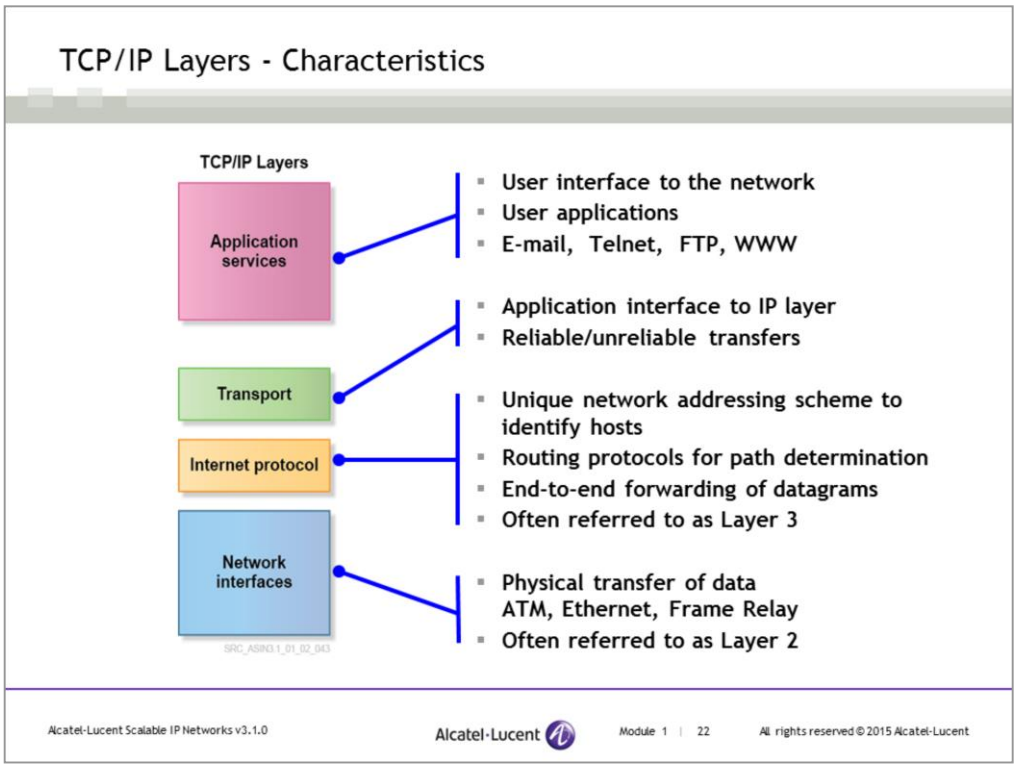
Internet protocol — The IP layer provides a universal and consistent forwarding service across a TCP/IP network. IP provides services that are comparable to the OSI network layer and is sometimes referred to as a Layer 3 (also known as L3) protocol.

Transport — The transport layer comprises two main protocols: TCP and UDP. These transport protocols provide services that are similar to the OSI transport protocols.

Application services — The application services provide end-user access to the Internet. Any of the services of the upper three OSI protocols that are required are incorporated into the application protocols.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The **application services** layer is where the user interfaces with the network. This layer applies only to network applications, such as e-mail, Telnet, FTP, and WWW. Without network connectivity, these applications would be useless. Applications such as word processors and database programs are not considered network applications because they do not require network connectivity.

The **transport layer** is the application's interface to the network. The transport protocol provides a mechanism for an application to communicate with another application that resides on another device in the network. In the TCP/IP suite, there are two transport protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

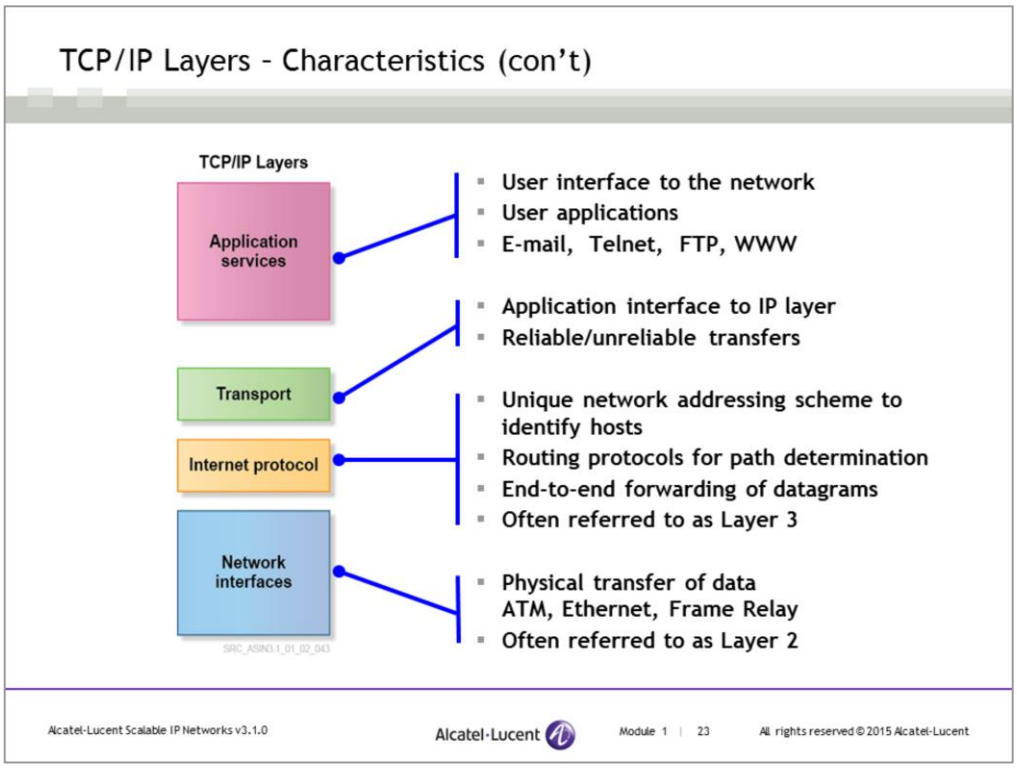
TCP is a connection-oriented protocol that provides an ordered and reliable transfer of data over the network.

UDP is a connectionless protocol that supports the transfer of a single datagram across the network with no delivery guarantee. UDP is simpler than TCP and operates with less overhead than TCP.

Most Internet applications, such as HTTP (hyper-text transfer protocol, used for web-browsing), email, Telnet, and File Transfer Protocol (FTP), use TCP for data transfer because it provides a reliable transfer service. Some applications, such as domain name system (DNS) and Simple Network Management Protocol (SNMP), use UDP because they only require a simple datagram transfer. Other applications, such as Real-time Transfer Protocol (RTP), use UDP to avoid the overhead of TCP, and because there is no benefit in the retransmission of lost packets for the applications that use RTP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The **Internet protocol** layer provides a common addressing plan for all hosts on the Internet, as well as a simple, unreliable datagram transfer service between these hosts. IP is the common glue that defines the Internet. IP also defines the way a datagram (or packet) is routed to its final destination. In an IP network, packet forwarding across the network is handled by routers. IP routers examine the destination address of a datagram and determine which router is the next hop that will provide the best route to the destination. The routers forward the packet to the next hop router, where the process is repeated until the datagram reaches its destination. This process is known as hop-by-hop routing.

Routers communicate with each other using dynamic routing protocols to exchange information about the networks to which they are connected. These topics are covered in greater detail in Modules 4 and 5. So far, the important point to remember is that routing protocols allow for delivery of packets from one router to the next in a predictable manner.

The Internet protocol layer is often referred to as Layer 3 because it provides open system interconnections (OSI) Layer 3-type services to the IP layer. For more information on the OSI model, please refer to ISO/IEC 7498-1.

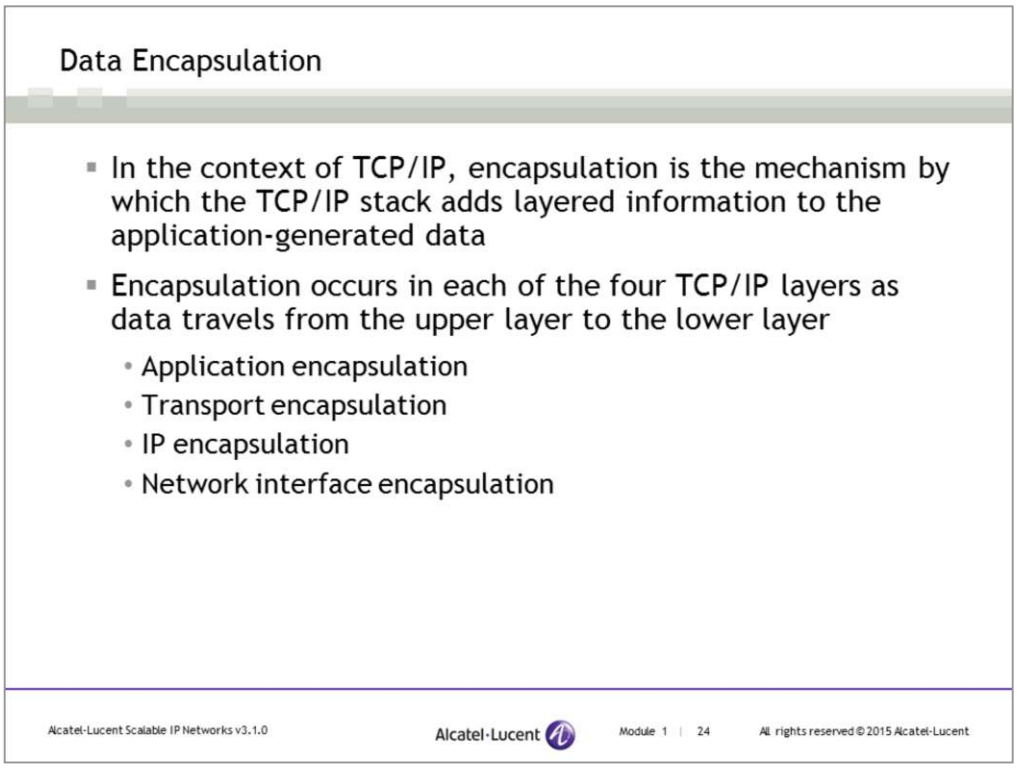
The **network interface** layer comprises the hardware that supports the physical interconnection of all network devices. The technologies of the network interface layer are often defined as multiple layers. The common trait of all technologies of this layer is that they can forward IP datagrams or packets.

There are many different technologies that operate at this layer, some of which are very complex. Some of the protocols commonly used at this layer include asynchronous transfer mode (ATM), frame relay, point-to-point protocol (PPP), and Ethernet. However, there are many other protocols used; some are open standard and some are proprietary.

The diversity of the network interface layer demonstrates one of the benefits of protocol layering. As new transmission technologies are developed, it is not necessary to change the upper layers in order to incorporate these technologies in the network. The only requirement is that the new technology be able to support the forwarding of IP datagrams. The network interface layer is often referred to as Layer 2 because it provides OSI Layer 2-type services to the IP layer. For more information on the OSI model, please refer to ISO/IEC 7498-1.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

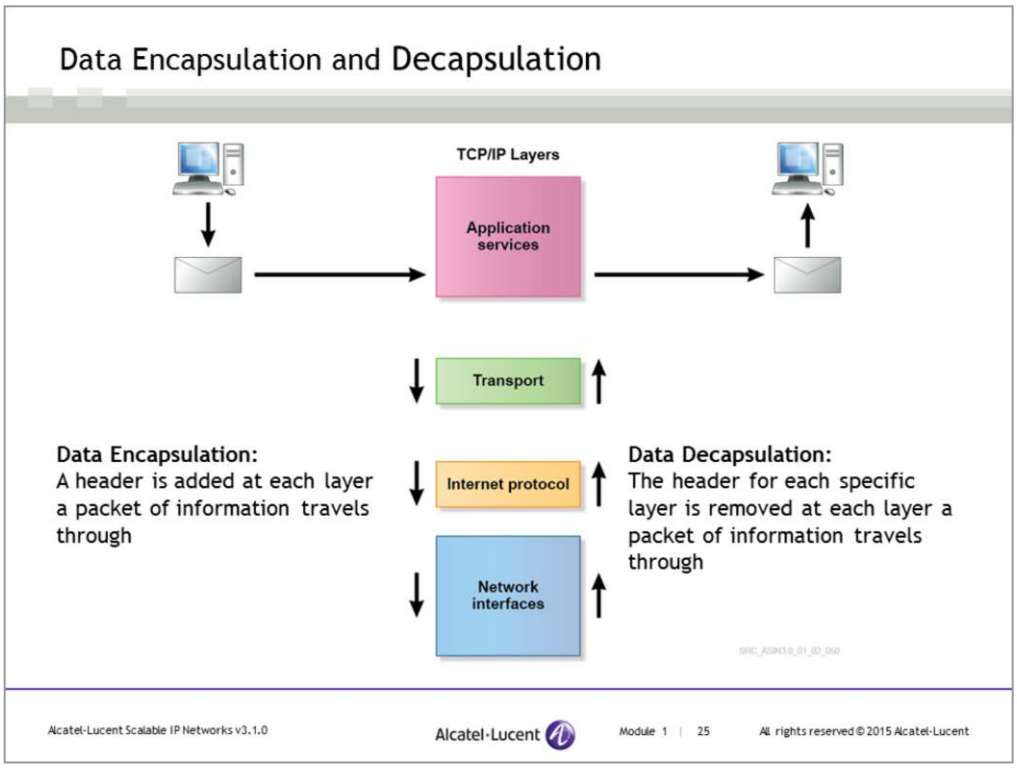


Data encapsulation, also known as data hiding, is the mechanism of hiding one data format within another data format. As the data travels from the TCP/IP upper layer to the lower layer, specific information, known as header, is added to the actual data.

The application layer generates the data, which is handed to the transport layer. The transport layer adds its overhead to the data, thereby hiding the original data. The data now is part of the transport layer and identified by the transport header. Similarly, once the transport data is received by the IP layer, the IP layer adds its overhead. At this point, the packet is referred to as an IP packet, thereby hiding the transport layer overhead and the application data. Finally, the IP layer needs the data link layer to perform the physical transmission of the IP packet. The network interface layer adds its own overhead to the IP packet and then transmits the data to the next router in the network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Each of the four TCP/IP layers performs a certain function.

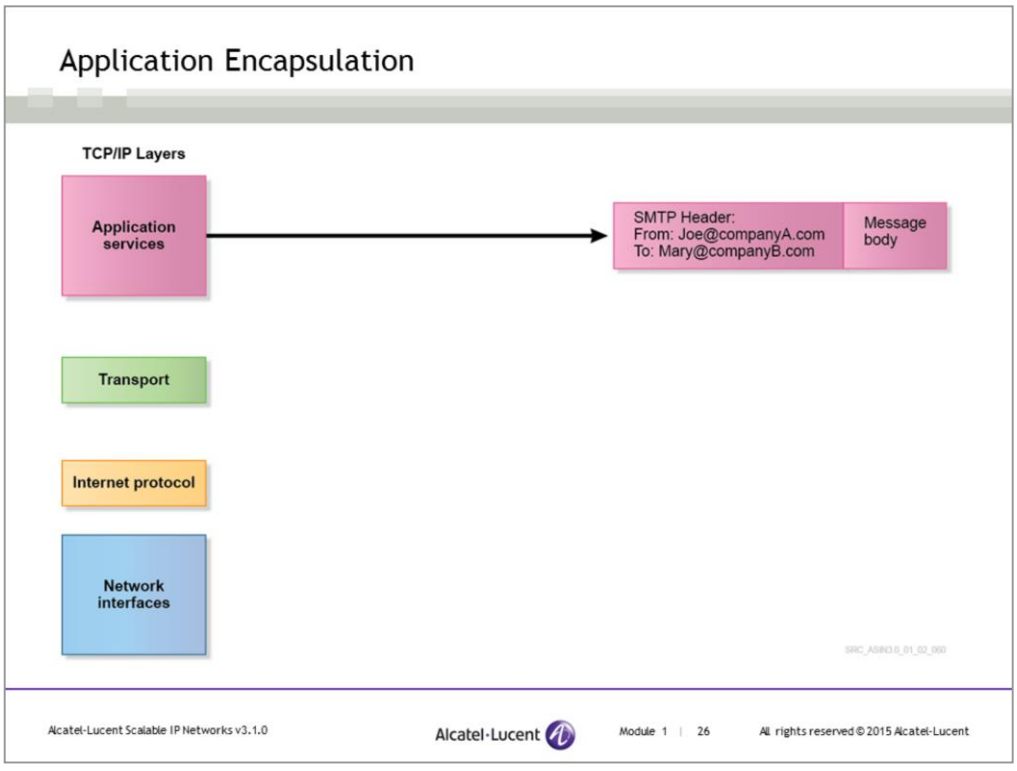
As data is sent from one computer, it will pass from the upper layer to the lower layer. A header is added at each layer a packet of information travels through. This is known as *encapsulation*.

On the receiving end, the data will then rebuild from the lower layer to the upper layer. The header for each specific layer is removed at each layer a packet of information travels through. This is known as *de-encapsulation (decapsulation)*.

The following slides will focus on encapsulation. De-encapsulation is simply the reverse of encapsulation.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When a network application needs to communicate with another application across the network, the application must first prepare its data in the specific format defined by the protocol to be used by the receiving application. A specific protocol is used so that the receiving application will know how to interpret the data it receives.

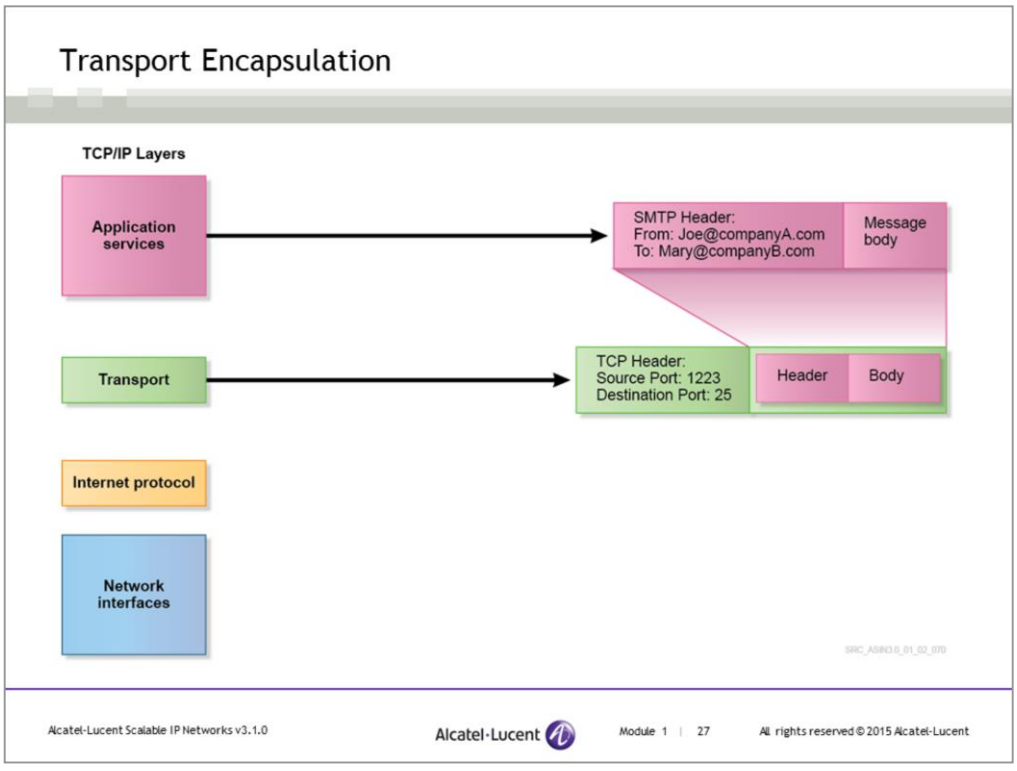
For example, an email application creates a message. An email message has two parts: the message header and the body. The message header contains the sender's and recipient's addresses, as well as other information such as the urgency of the message. The message body contains the contents of the email message. For the email application, a SMTP (Simple Mail Transfer Protocol) header is added.

In addition to defining the format of the message, the protocol also specifies how the applications are expected to interact with each other, including the exchange of commands and the expected responses.

The application uses the service of the transport layer to transfer its data.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The transport layer provides a service to transfer data between applications across a network. Two transport protocols are used on the Internet: TCP and UDP. To exchange email across the Internet, an email application uses SMTP. SMTP uses TCP to complete the transfer. TCP provides a reliable transfer service to ensure that all of the data is properly transferred.

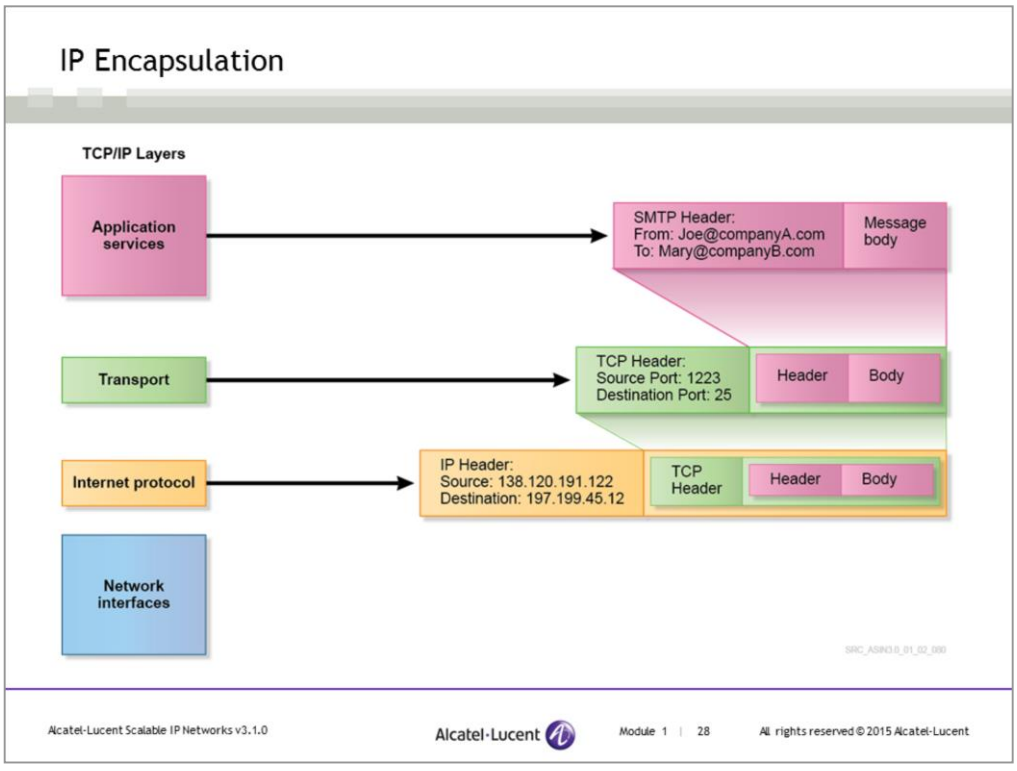
TCP treats all application data as a simple byte stream, including both the message header and the message body. TCP accepts the application's data and breaks it into segments for transmission across the network as required. To accomplish this reliable transfer, TCP packages the application data with a TCP header. On the receiving end of the connection, TCP removes the TCP header and reconstructs the application data stream exactly as the data was received from the application on the sender's side of the network. In other words, TCP simply takes the data received from the upper-layer application and passes it to the upper-layer application on the other end without trying to interpret the contents.

The TCP and UDP headers carry source and destination addresses that identify the sending and recipient applications because a single host system may support multiple applications. These addresses are known as port numbers. The port number 25 is used for SMTP.

To transmit data across the network, TCP uses the services of IP.

All rights reserved © 2015 Alcatel-Lucent.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The IP layer provides a common addressing scheme across the network, as well as a simple, unreliable datagram forwarding service between nodes in the network. Data from the transport layer is packaged in IP datagrams for transfer over the network.

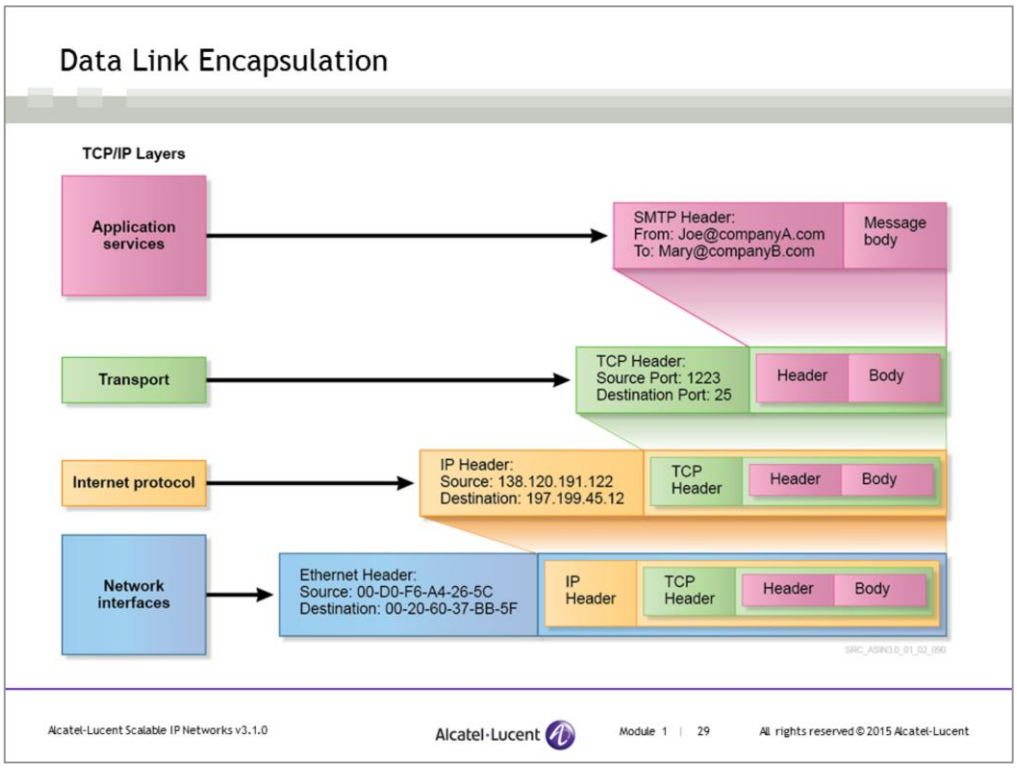
Each datagram travels independently across the network. The intermediate routers forward the datagram on a hop-by-hop basis based on the destination address. This allows for the network to dynamically route around any problems or failures in the network and deliver the packets as efficiently as possible.

Each datagram contains source and destination addresses that identify the end nodes in the network. Every node in an IP network is expected to have a unique IP address. IP uses the services of the underlying network interfaces to perform the physical transfer of data.

In this example, the Internet protocol layer adds source and destination IP addresses so that packets can be forwarded through the network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The data link layer is the term for the network interfaces that are used by IP to physically transmit the data across the network. The units of data transmitted at the data link layer are usually known as frames. IP datagrams must always be encapsulated in some type of data link frame for transmission.

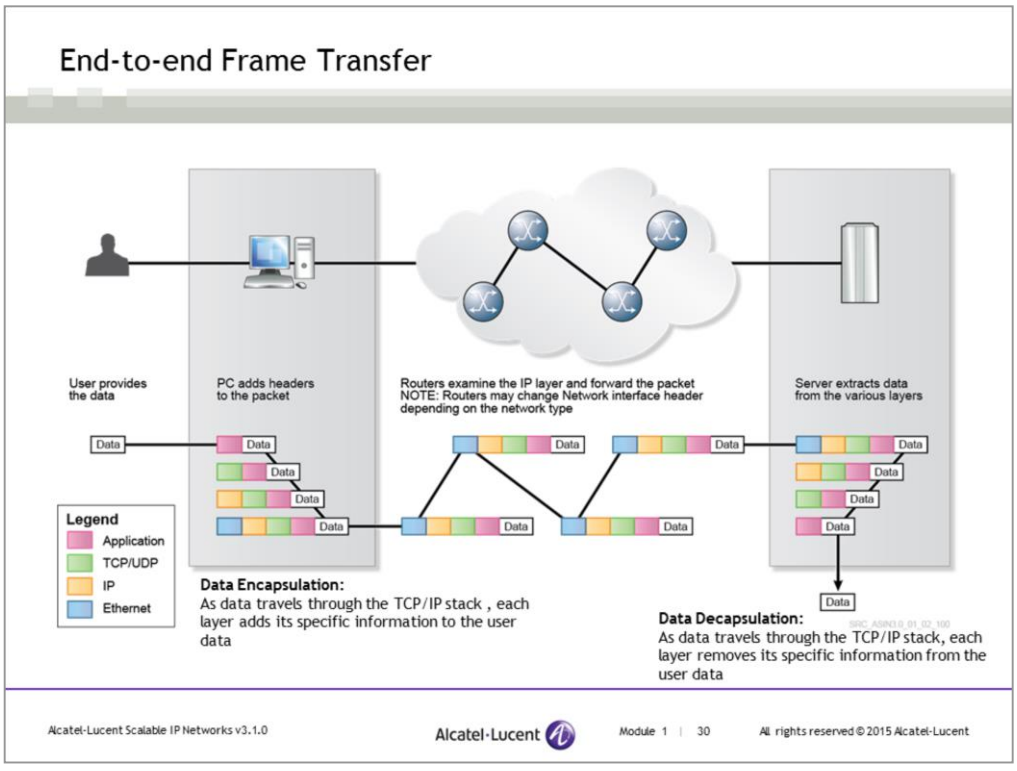
A typical data link frame contains a header, usually with an address. The frame may also contain a trailer with a checksum to verify the integrity of the transmitted data. There are many types of technologies used as network interfaces by IP. Each type of technology has its own specific format and rules of operation. The common characteristic is that all of these technologies carry IP datagrams.

Most protocols at this layer also use some form of addressing. The address is specific to the data link protocol and identifies the two endpoints of the data exchange.

For this example, the data link layer adds source and destination MAC addresses for forwarding on the local network segments.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Assume a user has composed and sent an email in his email application. Behind the scenes, the email application will take the data the user has written and place a SMTP protocol header in front of the data. The email application will then make a request to a TCP process running on the user's computer to send the SMTP information. TCP will accept the SMTP information and place a TCP header in front of the SMTP header. TCP then hands this information to the IP process. IP will place a IP header in front of the TCP header. After this, the IP process hands this information to the Ethernet process so that an Ethernet header (layer 2 header) is added in front of the IP information.

Now that all of the protocol headers have been inserted one after another, the packet is ready for transmission across the network. Each router along the path will:

- Remove the Ethernet header
- Read the IP header to determine the next hop router to forward the packet to
- Place a new Ethernet header onto the packet
- Forward the packet out of the interface toward the next hop router

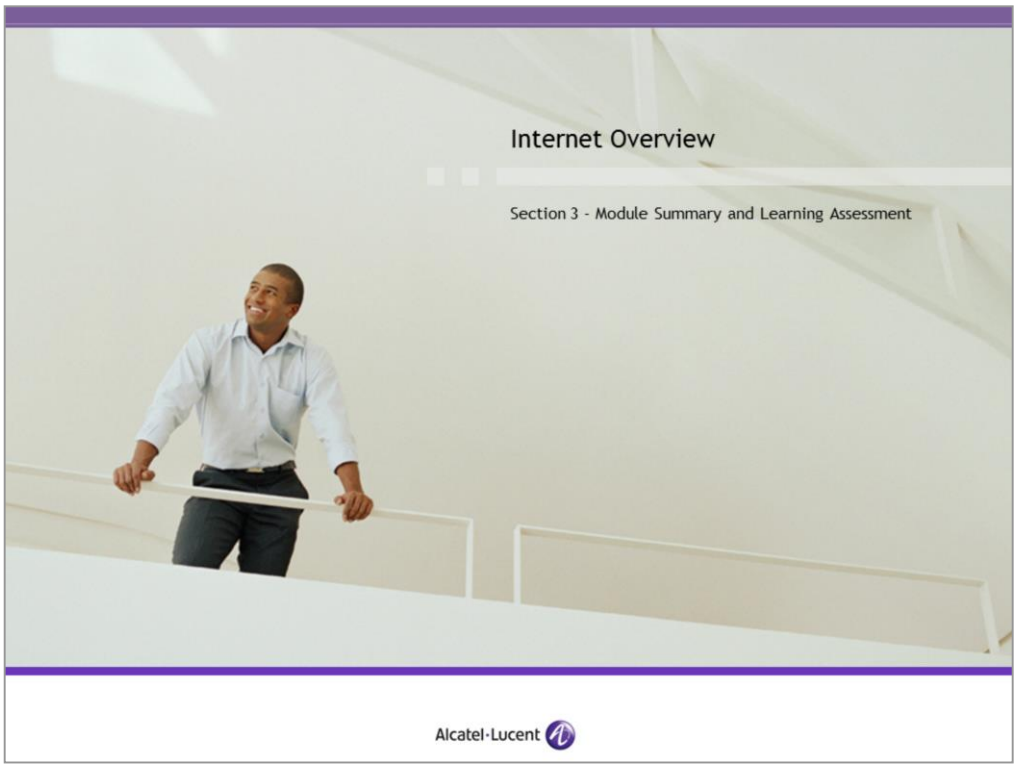
The layer 2 header is only used on a local network connection. Once the packet reaches the next hop router, the layer 2 information is no longer relevant. Therefore, a new layer 2 header is created and added to the packet. The packet is forwarded strictly based on the information in the IP header. None of the routers need to read the TCP header or SMTP header to forward the packets properly.

At the destination host, the processes described above are performed in the reverse order. Each process removes the appropriate header from the packets before passing it to the next process.

This slide shows how data is transferred from a source PC to a destination server across the Internet. Data from applications is sent to the TCP/IP protocol stack, where all appropriate headers are added and the packet is forwarded to the destination across the networks. As the data travels through the network, the layer 2 information (or the network interface layer information) is changed at each router, but the IP, transport, and application information remains unchanged. Once the data reaches the destination server, all headers will be removed and the data will be extracted.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Summary

- The Internet is a global system of interconnected networks
- Service providers offer connection to the Internet
- Content providers create or distribute content for the Internet
- Service providers can be classified into three tiers: Tier 1, Tier 2, and Tier 3, based on their size and functions
- IXPs allow various Tier 1, 2, and 3 providers to exchange Internet data.
- POPs are connection points between an ISP and its customers
- Modern ISPs can also be content providers or can connect to several content providers to provide a variety of services, mainly voice, video, and data applications

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 1 | 32
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Summary (con't)

- SLAs are contractual agreements between an ISP and its customers
- A demarcation point is the physical point at which ISP responsibility ends and customer responsibility begins
- TCP/IP is a suite of communication protocols used to connect hosts on the Internet
- TCP/IP layering provides a way to simplify a complex problem by segregating it into a number of smaller functions

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

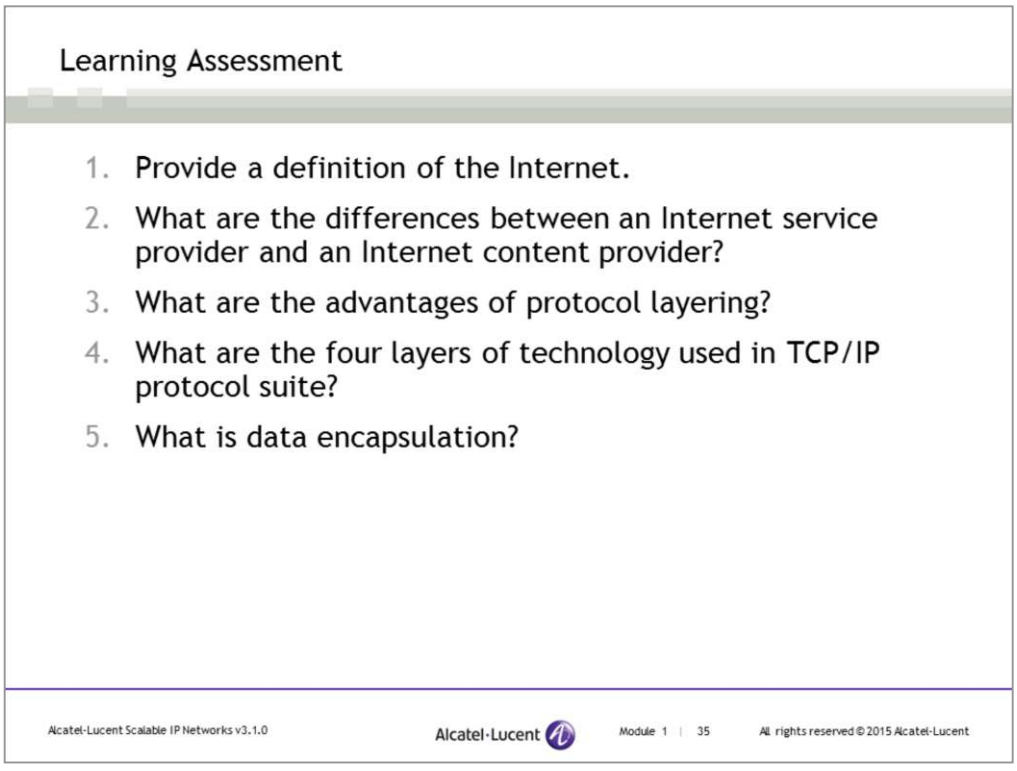
Module Summary (con't)

- TCP/IP is constructed with four layers of technology: application layer, transport layer, IP layer, and network interface layer
- At each layer, the data is encapsulated with a new header when the data travels from the upper layer to the lower layer
- As data travels back from the lower layer to the upper layer, a layer specific header is de-encapsulated from the data
- When data travels from one end to the other end, a new layer 2 header or network interface header is created at each router along the path
- A router uses IP header information to determine the next hop router to forward the packets

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 1 | 34
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

1. *Provide a definition of the Internet.*

   The Internet is global system of interconnected networks.

2. *What are the differences between an Internet service provider and an Internet content provider?*

   An Internet service provider provides Internet access to customers, while an Internet content provider creates or distributes online information.

3. *What are the advantages of protocol layering?*

   Protocol layering provides a way to simplify a complex problem by dividing it into a number of smaller functions. Each layer performs a specific function.

4. *What are the four layers of technology used in the TCP/IP protocol suite?*

   Application layer, transport layer, IP layer, and network interface layer.

5. *What is data encapsulation?*

   Data encapsulation, also known as data hiding, is the mechanism of hiding one data format within another data format. As the data travels from the TCP/IP upper layer to the lower layer, specific information, known as a header, is added along with the actual data.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Module Objectives

After successful completion of this module, you will be able to:

- Compare the functionality of Alcatel-Lucent's Service Router portfolio
- Describe the function of service router components
- Use CLI commands for configuration and verification
- Configure basic service router settings using CLI
- Configure and display event logs

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 2 | 2 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

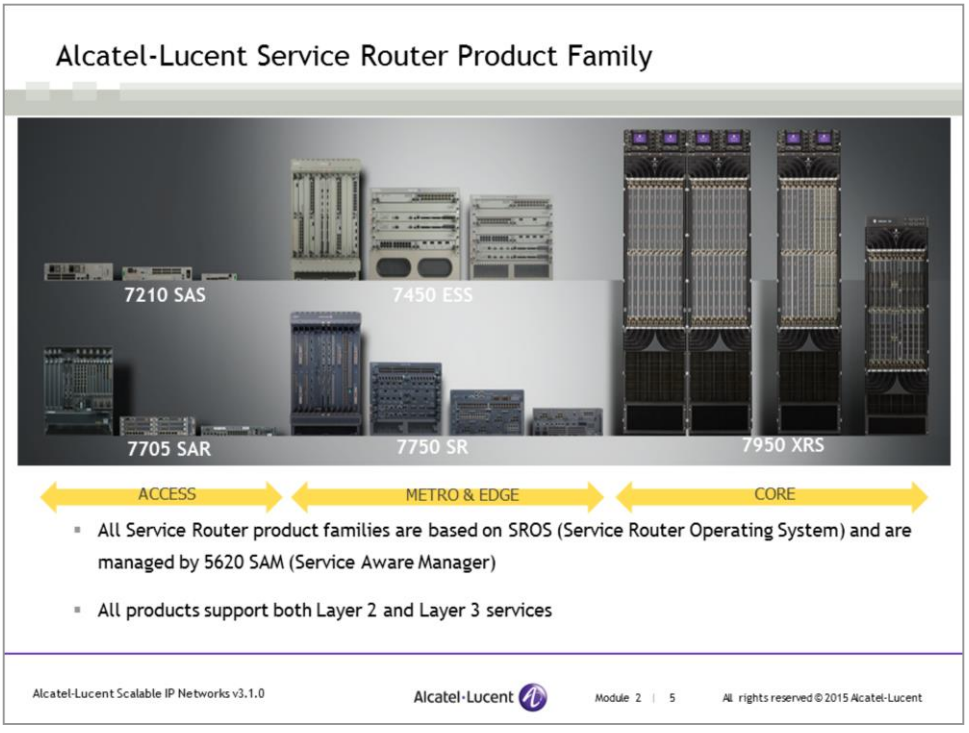
After successful completion of this section, you will be able to:

- List the Service Router suite of products
- Explain how different suites of products fit into a network topology

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 2 | 4 All rights reserved © 2015 Alcatel-Lucent



Alcatel-Lucent offers a complete IP routing portfolio that addresses the full service provider routing market from smallest POP (Point of Presence) to the largest ISP core.

The portfolio includes:

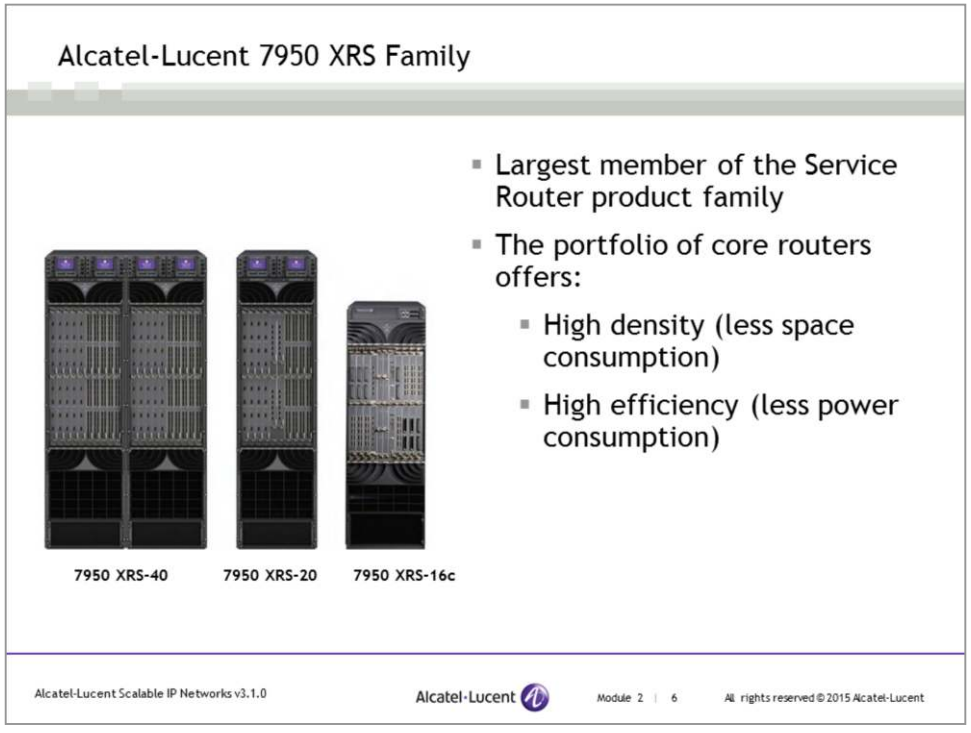
- Metro access (7705 SAR and 7210 SAS), Metro aggregation (7450 ESS and 7750 SR) and IP Edge (7750 SR)
- Metro core (7750 SR and 7950 XRS) and IP core routing (7950 XRS) platforms.

All Service Router product families are built around the proven, resilient, and feature-rich SR-OS (Service Router Operating System). All product families are fully managed by the 5620 SAM (Service Aware Manager) resulting in integrated network management end-to-end.

Each product family has different chassis variants that can be deployed to perform a wide range of functions.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Alcatel-Lucent 7950 XRS is a powerful core IP/MPLS routing platform, based on the same SR OS as other service routers in other product families. Key characteristics include:

- Meets service provider's needs for core routing, Internet peering, MPLS switching, datacenter interconnection and infrastructure services such as VLL (Virtual Leased Line) and VPN (Virtual Private Network) in a single platform
- Supports capabilities aimed to minimize service disruption, including non-stop routing, stateful failover of protocols, and in-service software upgrades (ISSUs), along with service assurance and monitoring tools across IP, MPLS, and Ethernet domains
- Versatility to address current and future requirements of IP backbone and metro core networks
- High density - takes one fifth of space compared to traditional platforms
- High efficiency - consumes one third of power compared to traditional platforms

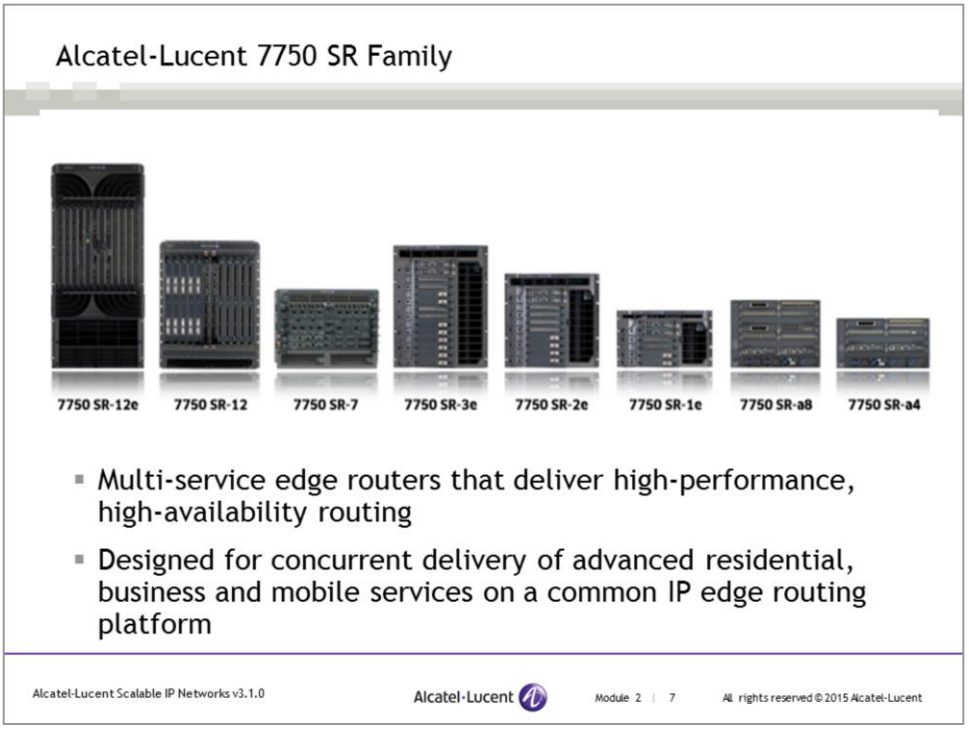
Please see *Alcatel-Lucent 7950 Extensible Routing System Release 13* for more information on the 7950 XRS.

Chassis variants as of 7950 XRS Release 13 (not tested on ASIN exam):

- 7950 XRS-40
- 7950 XRS-20
- 7950 XRS-16c

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Alcatel-Lucent 7750 SR is a multi-service edge router, based on the same SR OS as other service router product families. Key characteristics include:

- Delivers advanced residential, business, and mobile services on a common IP edge routing platform
- Deploys for a wide range of functions, including:
  - Broadband network gateway for residential service delivery with advanced subscriber management
  - Multiservice edge router for business VPN/Internet access, cloud and data center interconnect services
  - Enterprise router providing intelligent connectivity to the cloud, data center, Internet, and branch offices
  - Mobile backhaul aggregation router to address the needs of macro, small cell and heterogeneous networks
  - Mobile gateway for the mobile packet core (2G, 3G, and LTE)
  - WLAN gateway for carrier Wi-Fi networks supporting Wi-Fi mobility
  - Security gateway for macro, small cell and carrier Wi-Fi networks
- Supports capabilities aimed to minimize service disruption, including non-stop routing, non-stop services, stateful failover of protocols, in-service software upgrades (ISSUs), fast reroute, pseudowire redundancy, along with service assurance and monitoring tools across IP, MPLS, and Ethernet domains

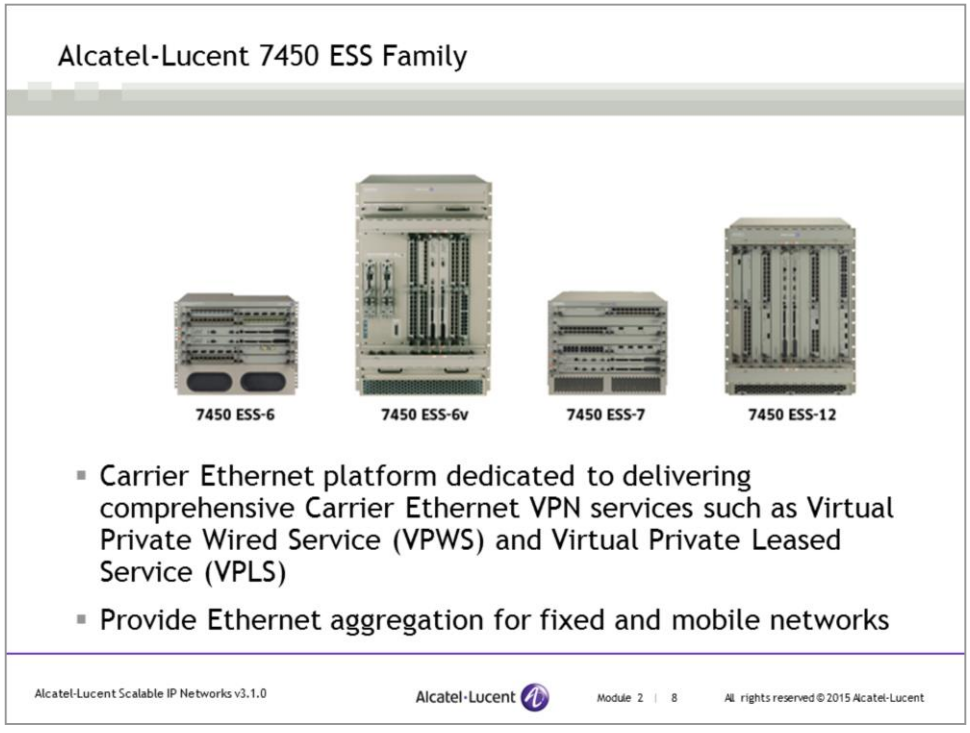
Please see *Alcatel-Lucent 7750 Service Router Release 13* for more information on 7750 SR.

Chassis variants as of 7750 SR Release 13 (not tested on ASIN exam):

- 7750 SR-12e, 7750 SR-12, 7750 SR-7, 7750 SR-3e, 7750 SR-2e, 7750 SR-1e, 7750 SR-a8, 7750 SR-a4, 7750 SR-c4, 7750 SR-c12.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Alcatel-Lucent 7450 ESS is a Carrier Ethernet Switch Platform, based on the same SR OS as other service router product families. Key characteristics include:

- Provides comprehensive Carrier Ethernet and IP/MPLS feature support
- Provides metro Ethernet aggregation for fixed and mobile networks
- Offers any combination of value added Ethernet or IP-based services in a highly scalable platform
- Supports capabilities aimed to minimize service disruption, including non-stop routing, non-stop services, in-service software upgrades (ISSUs), fast reroute, pseudowire redundancy, along with service assurance and monitoring tools across IP, MPLS, and Ethernet domains

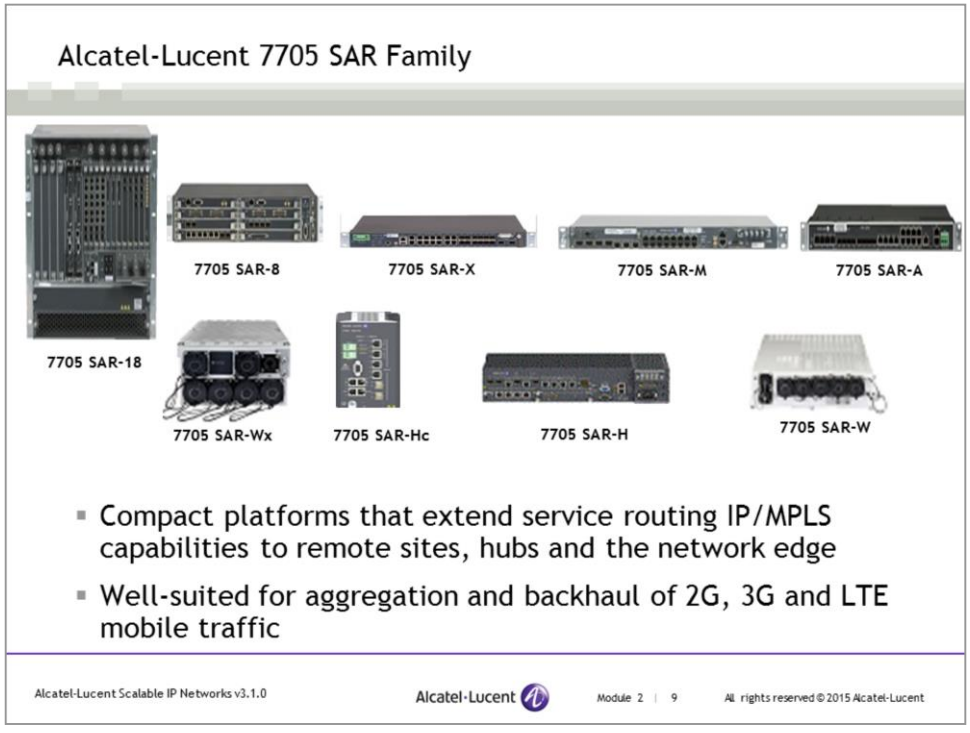
Please see *Alcatel-Lucent 7450 Ethernet Service Switch Release 13* for more information on 7450 ESS.

Chassis variants as of 7450 ESS Release 13 (not tested on ASIN exam):

- 7450 ESS-12
- 7450 ESS-7
- 7450 ESS-6V
- 7450 ESS-6

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Alcatel-Lucent 7705 SAR is used for multiservice adaptation, aggregation and routing, especially onto a modern Ethernet and IP/MPLS infrastructure, based on the same SR OS as other service router product families. Key characteristics include:

- Compact, low-power consumption platform
- Indoor and outdoor platforms that deliver highly available services over resilient and flexible network topologies
- Suited for aggregation, backhaul and routing of 2G, 3G, and LTE mobile traffic
- Resiliency and redundancy, including hitless control and switch failover, synchronization redundancy, network uplink resiliency and power feed redundancy

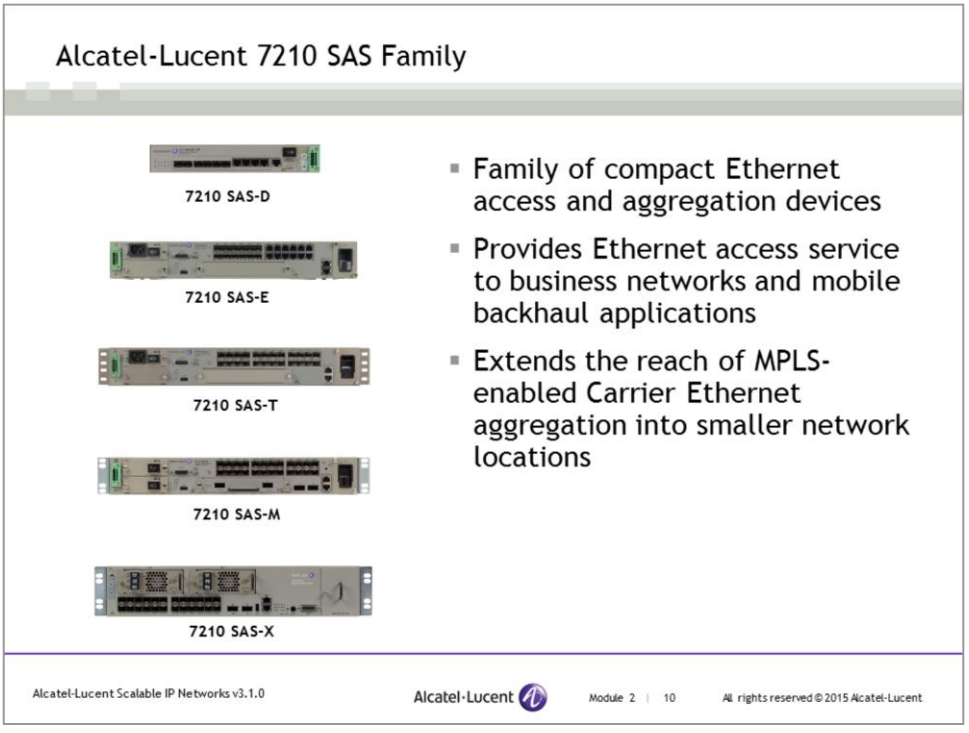
Please see *Alcatel-Lucent 7705 Service Aggregation Router Release 7.0* for more information on 7705 SAR.

Chassis variants as of 7705 SAR Release 7.0 (not tested on ASIN exam):

- 7705 SAR-18
- 7705 SAR-8
- 7705 SAR-H
- 7705 SAR-M
- 7705 SAR-A
- 7705 SAR-X
- 7705 SAR-W
- 7705 SAR-Wx
- 7705 SAR-Hc

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Alcatel-Lucent 7210 SAS is a portfolio of compact Ethernet access and aggregation devices, based on the same SR OS as other service router product families. Key characteristics include:

- Delivers Carrier Ethernet demarcation in support of business networking services or mobile cell site gateway applications
- Extends the reach of Ethernet and Multiprotocol Label Switching (MPLS)-enabled Carrier Ethernet aggregation into smaller network locations

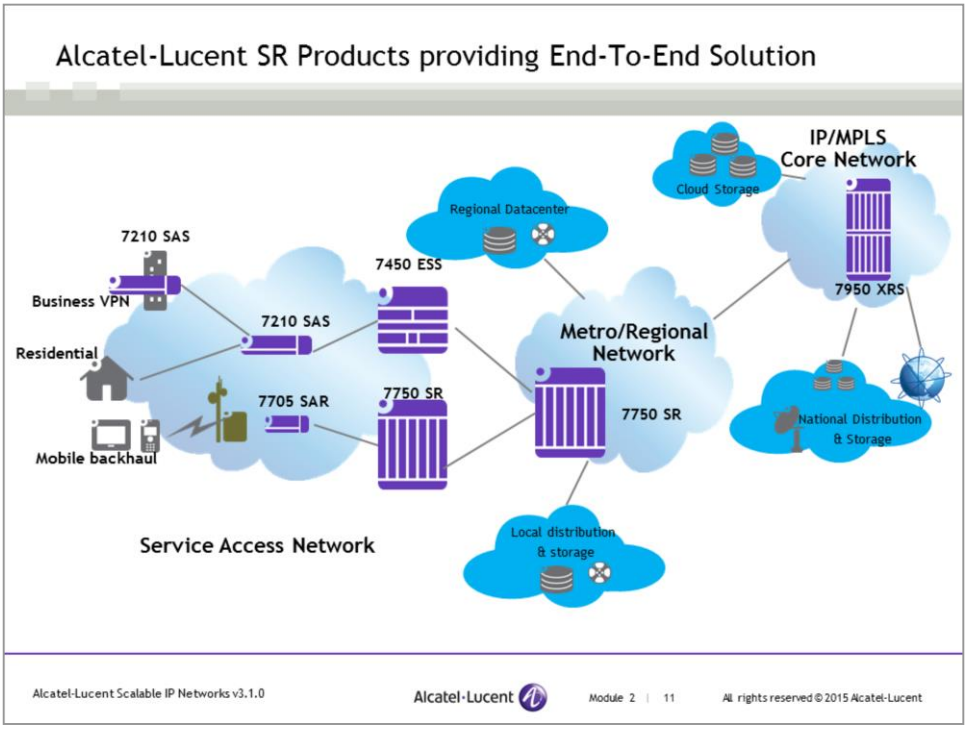
Please see *Alcatel-Lucent 7210 Service Access Switch Release 8.0* for more information on 7210 SAS.

Chassis variants as of 7210 SAS Release 8.0 (not tested on ASIN exam):

- 7210 SAS-D
- 7210 SAS-E
- 7210 SAS-T
- 7210 SAS-M
- 7210 SAS-X
- 7210 SAS-R6
- 7210 SAS-K

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the wide range of Alcatel-Lucent SR products used to provide an end-to-end solution.

At the service access network, there is 7210 SAS, 7705 SAR and 7450 ESS.

The 7210 SAS is a CPE device that provides Carrier Ethernet service for a business network. It is also an Ethernet access and aggregation device that provides low-cost MPLS aggregation in smaller network locations (business and residential).

The 7705 SAR is a cell site aggregation router, providing aggregation for 2G, 3G, and LTE mobile backhaul over a modern IP/MPLS network.

The 7450 ESS is an Ethernet access aggregation device, providing higher capacity MPLS aggregation for the metro Ethernet aggregation fixed and mobile networks.

The 7750 is an IP edge router in a metro/regional network to support concurrent delivery video, voice, mobile and data applications.

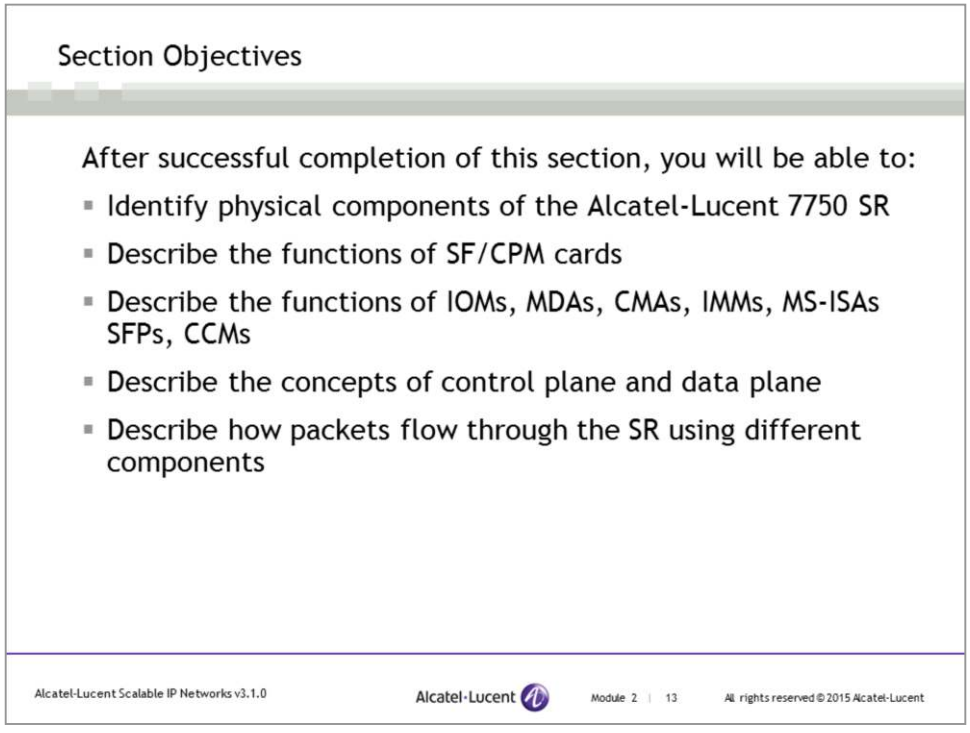
The 7950 XRS is a powerful IP backbone and metro core router in the IP/MPLS core network, providing high density and efficiency while supporting growing demand for bandwidth.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

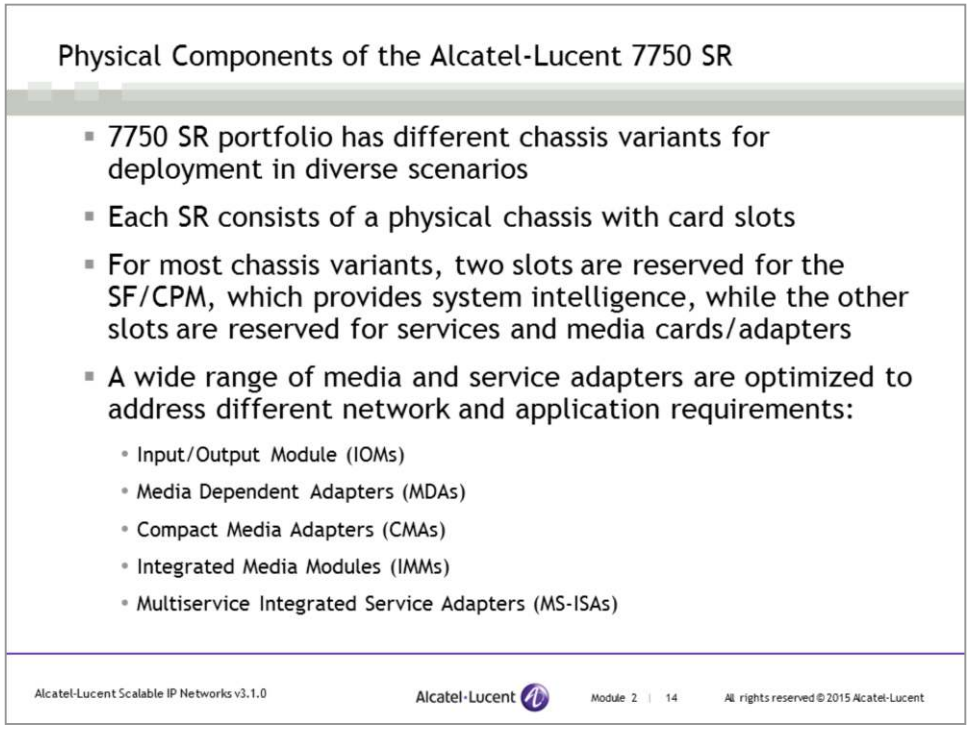
 All rights reserved © 2015 Alcatel-Lucent



The focus of this course is the Alcatel-Lucent 7750 SR.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



As of Alcatel-Lucent's 7750 SR Release 13, the 7750 SR is available in eight chassis variants: 7750 SR-12e, SR-12, SR-7, SR-3e, SR-2e, SR-1e, SR-a8 and SR-a4. The eight-variant family has the capacity to address the smallest to largest network locations.

There are a wide range of media and service adapters optimized to address different network and application requirements:

Input/Output Modules (IOMs) – Responsible for queuing, processing and forwarding data

Media Dependent Adapters (MDAs) – Provides physical interface connectivity

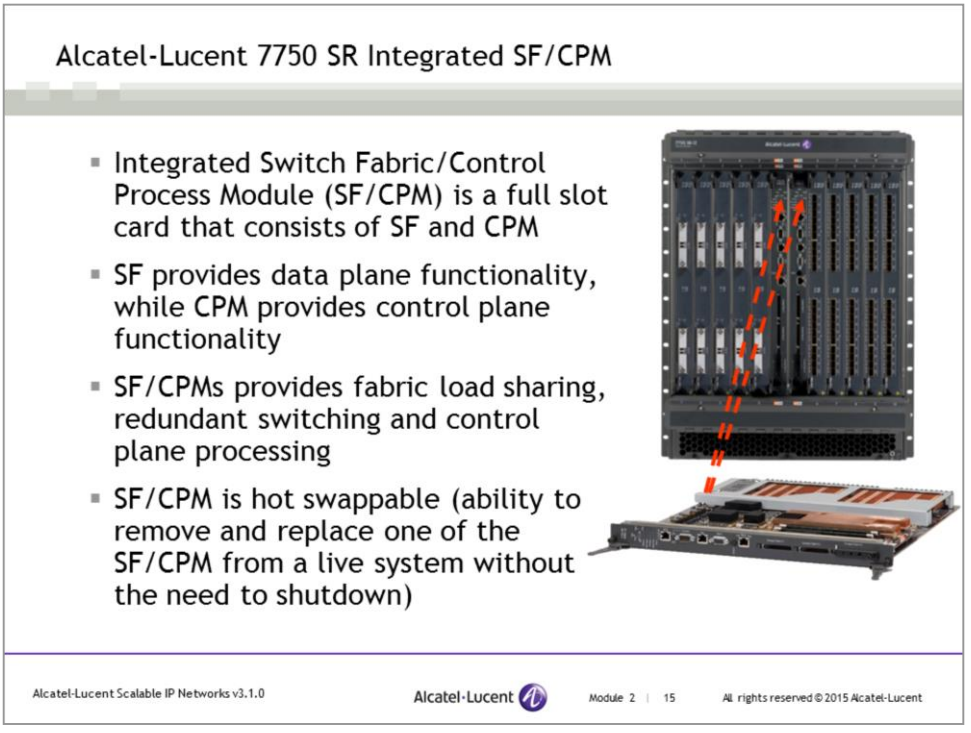
Compact Media Adapters (CMAs) – Supports lower-speed services and port densities

Integrated Media Modules (IMMs) – Provides integrated processing and physical interfaces on a single board

Multiservice Integrated Service Adapters (MS-ISAs) – Resource adapters that provide specialized processing and buffering for applications

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



The Integrated SF/CPM (Switch Fabric/Control Processor Module) provides data plane and control plane functionality.

SF provides data plane functionality, while CPM provides control plane functionality.

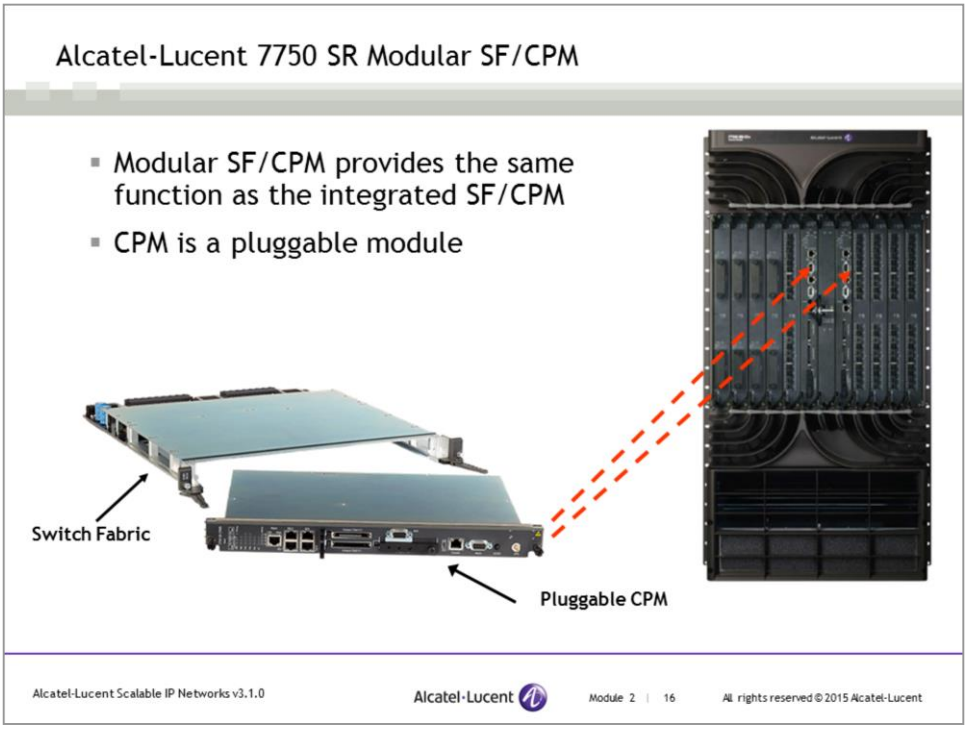
The SF/CPM is 1+1 redundant with a dual, active load sharing design. Redundant SF/CPMs operate in a hitless, stateful failover mode.

SF/CPM is a hot-swappable module. The term hot-swappable refers to the ability to remove and replace one of the SF/CPM from a live system without the need to shutdown.

Integrated SF/CPM can be housed in 7750 SR-7, 7750 SR-12, and 7750 SR-12e.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

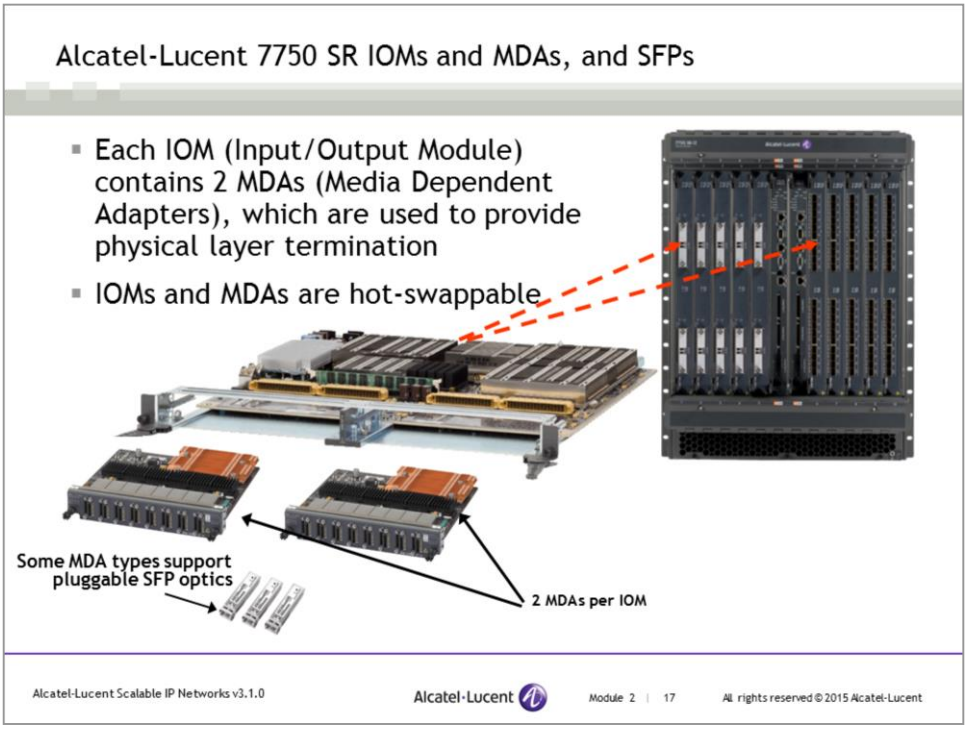


The Switch Fabric Module (SFM5-12e) is a full-height card used in a 7750 SR-12e chassis.

The Control Processor Module (CPM5) is a pluggable module housed within the SFM5-12e. The CPMs are 1+1 redundant with a dual, active load sharing design. Redundant CPMs operate in a hitless, stateful failover mode.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IOMs (Input/Output Modules)

IOMs are hot-swappable modules that connect to standard physical interfaces. IOMs contain two traffic-processing programmable fast path complexes. Each complex supports a pluggable MDA that allows a common programmable fast path to support all of the possible interface types. Each IOM also contains a CPU section to manage the forwarding hardware in each flexible fast path. IOM can also be used to house Integrated Service Adapters (ISAs).

The term hot-swappable refers to the ability to remove and replace an IOM from a live system without the need to shutdown. However, replacing IOM will affect the MDA connectivity.

As of 7750 SR Release 13, IOMs are supported on the 7750 SR-12e, SR-12 and SR-7 platforms.

MDAs (Media Dependent Adapters)

MDA is a hot-swappable, half-slot card providing physical layer termination. MDAs are available in a variety of interfaces such as Ethernet, POS (Packet of SONET/SDH), ATM, ASAP (Any Services Any Port), TDM, and CES (Circuit Emulation Services). MDAs pass incoming frames to the IOM for processing, and transmit outgoing frames to the appropriate physical interface in the correct format.

The term hot-swappable refers to the ability to remove and replace an MDA from a live system without the need to shutdown.

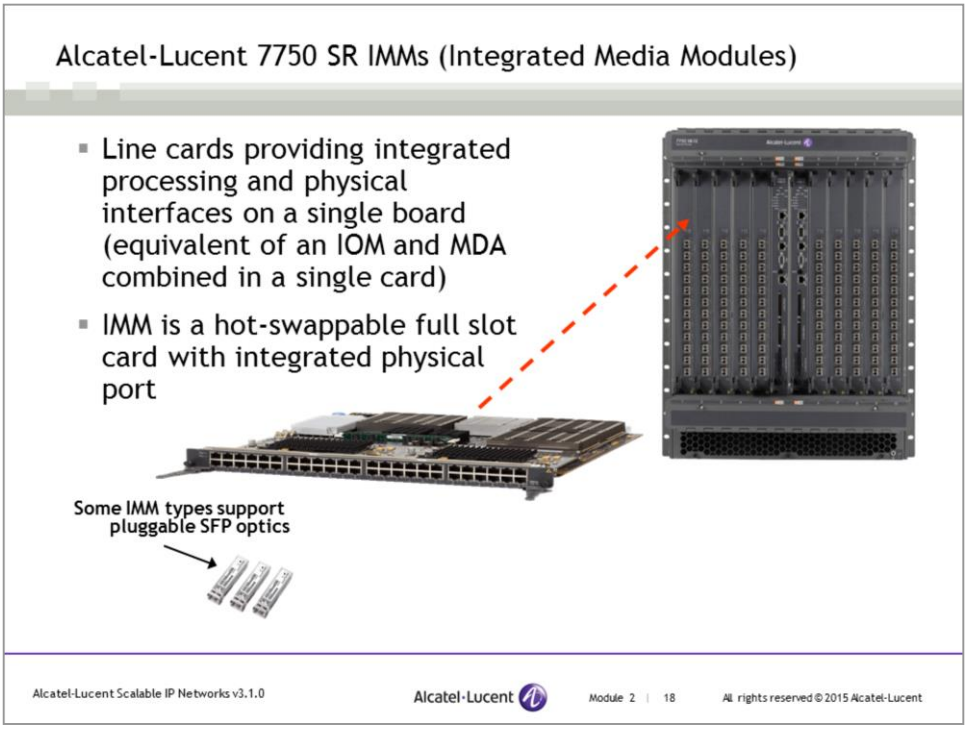
MDAs are supported on all platforms.

SFP interfaces

SFPs transceivers are small, optical modules available in a variety of formats. Not all MDA types support removable SFP optics.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



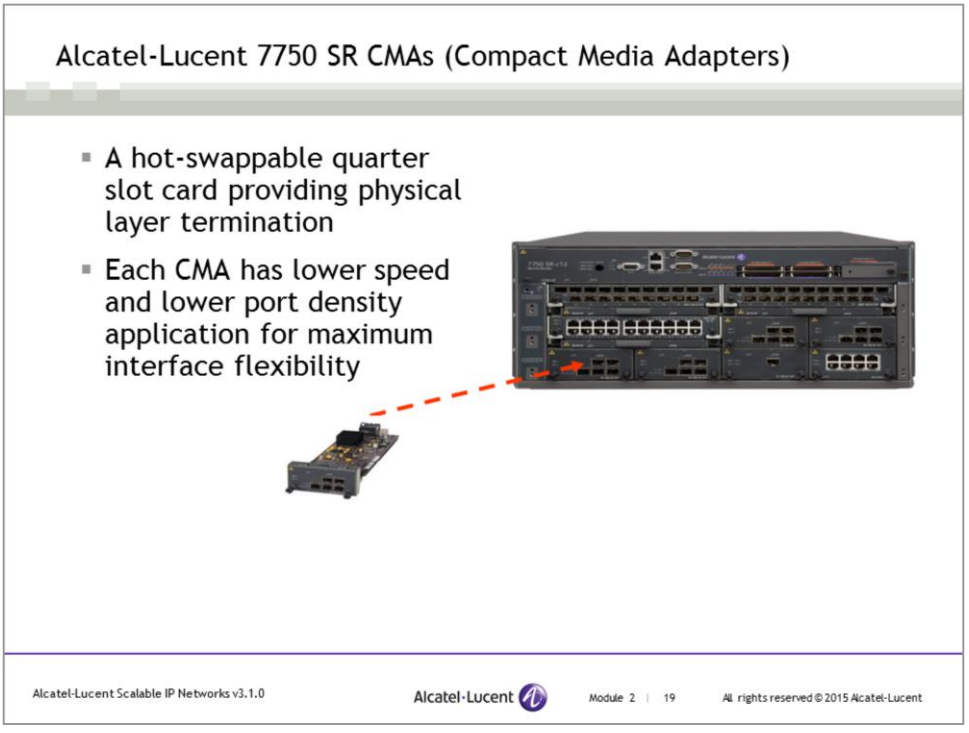
IMMs (Integrated Media Modules)

IMMs are hot-swappable, full-slot line cards providing integrated processing and physical interfaces on a single board. IMMs provide high-capacity, high-density Ethernet and SDH/SONET interfaces. The term hot-swappable refers to the ability to remove and replace an IMM from a live system without the need to shutdown.

As of 7750 SR Release 13, IMMs are supported on the 7750 SR-12e, SR-12 and SR-7 platforms.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



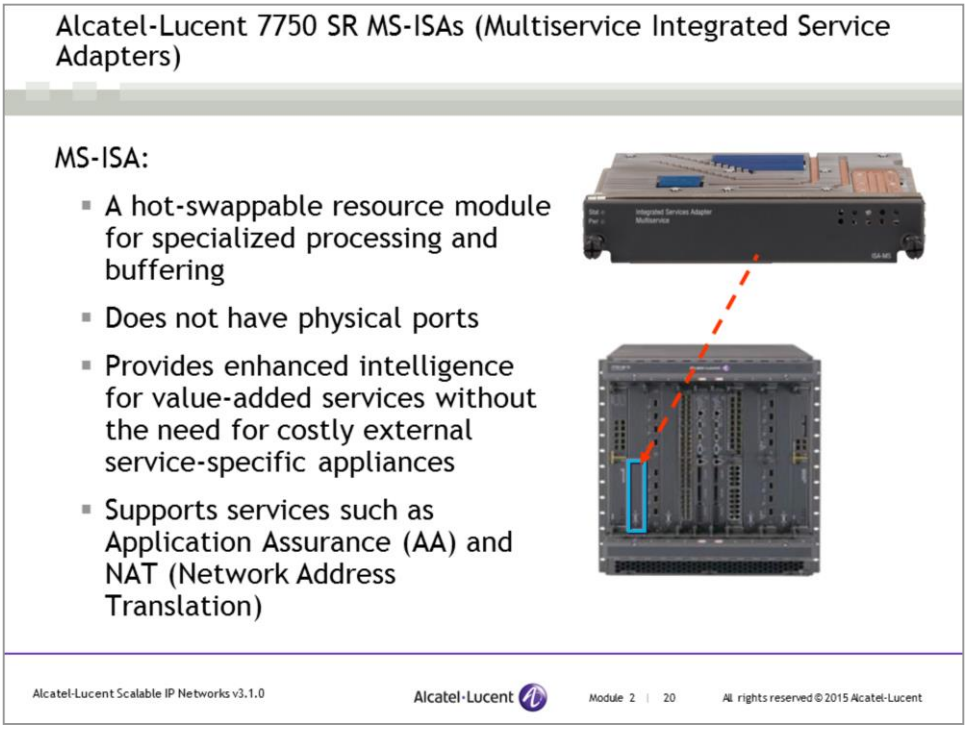
CMAs (Compact Media Adapters)

CMAs are hot-swappable quarter-slot cards providing physical layer termination. CMAs are interface adapters supporting lower speed and port density than MDAs. This provides maximum interface flexibility because up to four different CMAs can be supported in a single slot. The term hot-swappable refers to the ability to remove and replace a CMA from a live system without the need to shutdown.

As of 7750 SR Release 13, CMAs are supported on the 7750 SR-c12 and SR-c4 platforms.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



MS-ISAs (Multiservice Integrated Adapters)

MS-ISAs are hot-swappable resource adapters that are slotted into IOMs. MS-ISAs provide specialized processing and buffering for applications. The term hot-swappable refers to the ability to remove and replace a MS-ISA from a live system without the need to shutdown.

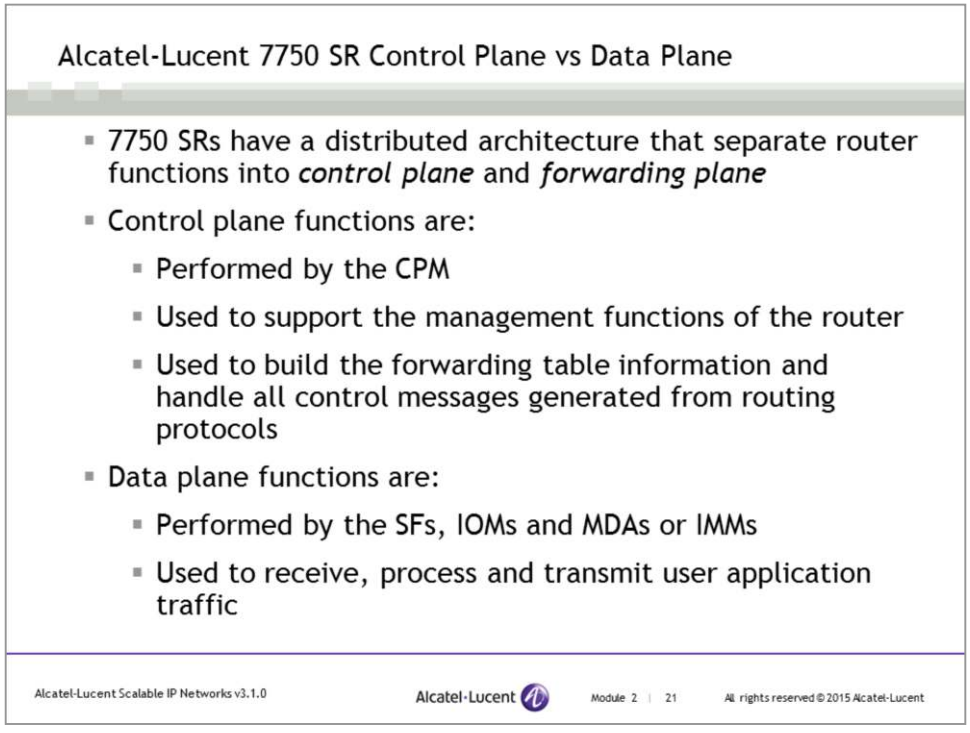
MS-ISA is a high capability module that provides enhanced intelligence for value-added services without costly external service-specific appliances. Different ISA types are used to support different applications.

- Application Assurance (AA) for application-aware Quality of Service (QoS) and performance measurement
- Broadband extensions: Network Address Translation and Dual Stack-Lite for allowing IPv4 and IPv6 services to run across a single IPv6-only access network. The NAT function offered by the MS-ISA card is normally referred to as CG-NAT or Carrier Grade Network Address Translation.
- Tunnel: IPSec for providing high performance and scalable encryption

MS-ISAs are supported on all platforms.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Modern routers such as 7750 SR have a distributed architecture that separates router functions into control plane and forwarding plane actions.

In the 7750 SR, the control plane functions are performed by the SF/CPM (switch fabric/control plane module), and the forwarding plane functions are performed by the IOM cards. The separation of the data plane processing from the control plane processing ensures the 7750 SR can be managed even when there are extremely high volumes of user data traffic.

Control plane functions

The control plane has two main functions:

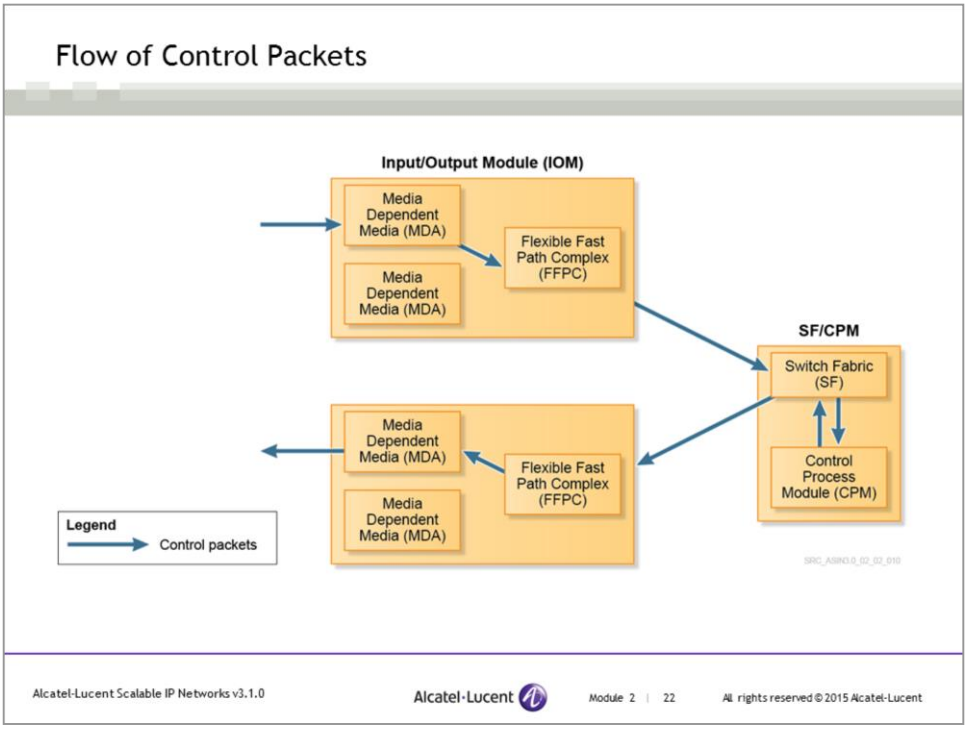
- Supporting the management functions of the router through the Command Line Interface (CLI) and network management capabilities. This includes configuration and administration of the router.
- Building the forwarding table for the IOM. The forwarding table is constructed from the routing table, which is built through the operation of dynamic routing protocols and/or configured with static routes. More information about how the forwarding table is built is discussed in Module 5.

Data plane functions

The data plane functions occur after the control plane has built the forwarding information and stored the data in the IOM. The IOM cards have the intelligence and information required to forward IP packets without any involvement from the control plane. The forwarding complex on the IOM contains memory and processors that enable it to receive, process and transmit user application packets at wire speeds.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



This slide shows the flow of control plane packets through various components within an Alcatel-Lucent 7750 SR. A control packet contains routing and management information and it is intended for the CPM (Control Processor Module). The control plane functions are performed by the CPM.

Note that in the IOM3 architecture shown in this slide, a single FFPC is shared between the two MDAs.

Control Packet Flows

The following steps are control packet flows when packets are received by the Alcatel-Lucent 7750 SR.

1. A control packet from the remote network/customer site ingresses through the MDAs, where the data is converted into a proprietary internal format.
2. The packet is then processed in the I/O module (IOM) where the forwarding decision occurs (using a forwarding table lookup).
3. When the next-hop or egress interface for the packet is known, the packet is sent to the switch fabric.
4. Since the packet is a control packet, the packet is sent to CPM for processing.
5. The packet is then sent to the appropriate IOM and MDA associated with the egress interface.
6. The egress MDA also converts the internal format into the appropriate interface format.

Ingress flexible fast path complex (FFPC) is responsible for:

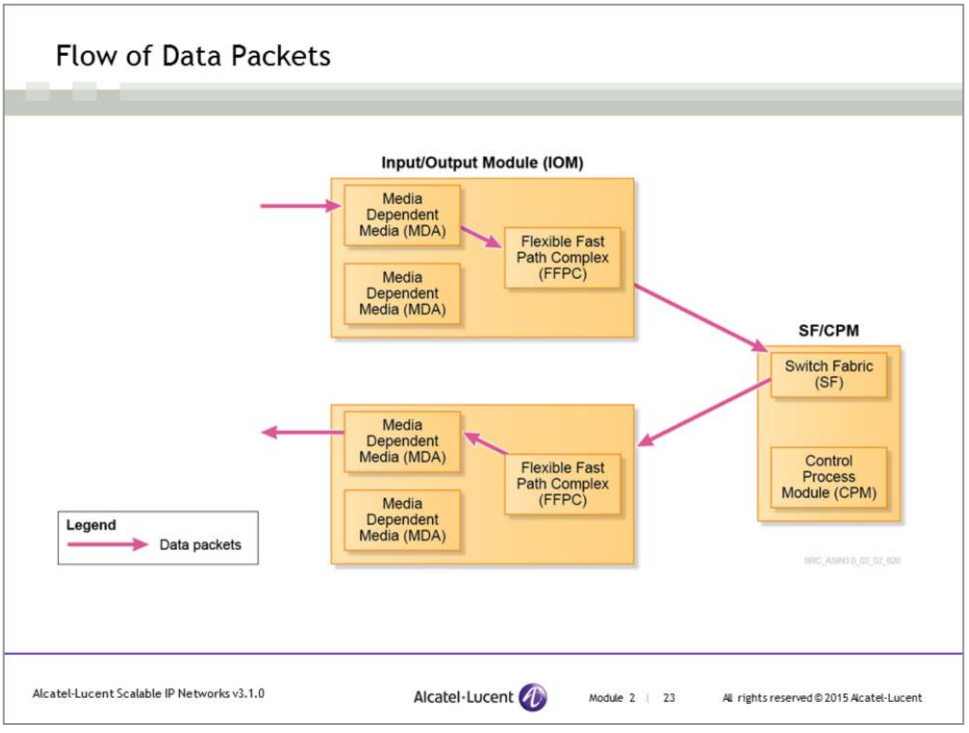
- Applying Quality of service to classify and treat packets differently, including buffering
- Determining forwarding destination (the destination IOM/MDA/port)

Egress flexible fast path complex (FFPC) is responsible for:

- QoS classification and buffer management for egressing data

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the flow of data plane packets through various components within an Alcatel-Lucent 7750 SR. A data packet is user data intended for an application such as email or file transfer. The data plane operations are performed by the IOM card.

Note that in the IOM3 architecture shown in this slide a single FFPC is shared between the two MDAs.

Data Packet Flows

The following steps are data packet flows when packets are received by the Alcatel-Lucent 7750 SR.

1. A data packet from the remote network/customer site ingresses through the MDAs, where the data is converted into a proprietary internal format.
2. The packet is then processed in the I/O module (IOM) where the forwarding decision occurs (using a forwarding table lookup).
3. When the next-hop or egress interface for the packet is known, the packet is sent to the switch fabric.
4. The packet is then sent to the appropriate IOM and MDA associated with the egress interface.
5. The egress MDA also converts the internal format into an appropriate interface format.

Ingress flexible fast path complex (FFPC) is responsible for:

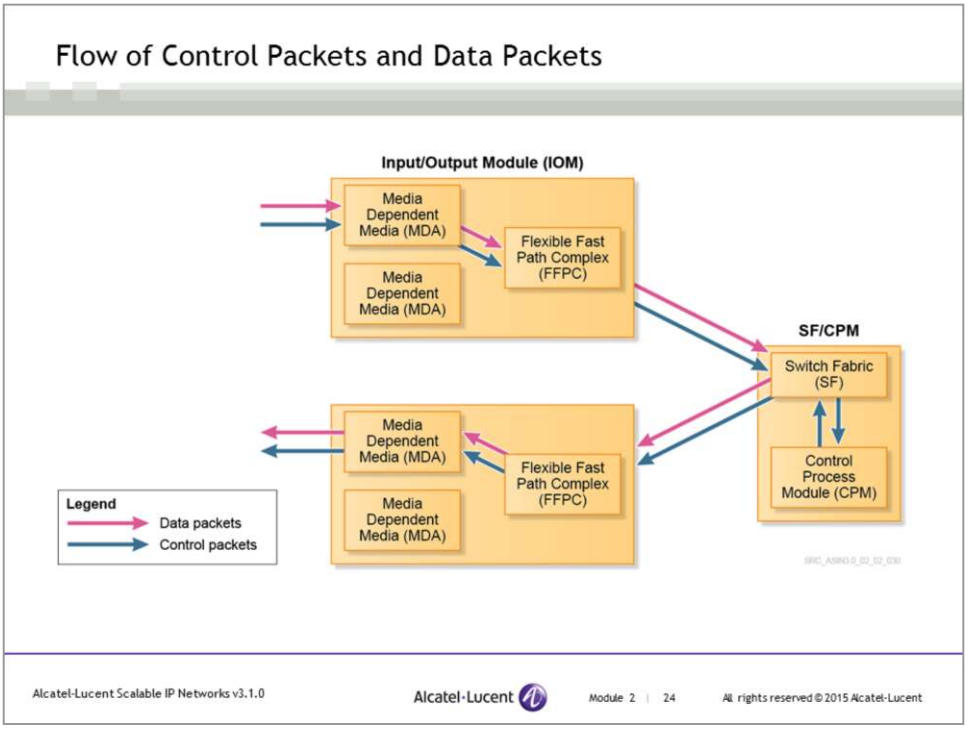
- Applying Quality of service to classify and treat packets differently, including buffering
- Determining the forwarding destination (destination IOM/MDA/port)

Egress flexible fast path complex (FFPC) is responsible for:

- QoS classification and buffer management for egressing data

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the flow of data plane packets and control plane packets through the Alcatel-Lucent 7750 SR. A data packet is user data intended for an application such as email or file transfer. Control packet contains routing and management information intended for the CPM. This separation of the user data packet processing from the protocol control data packet processing ensures the 7750 SR can be managed even when there are extremely high volumes of user traffic.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

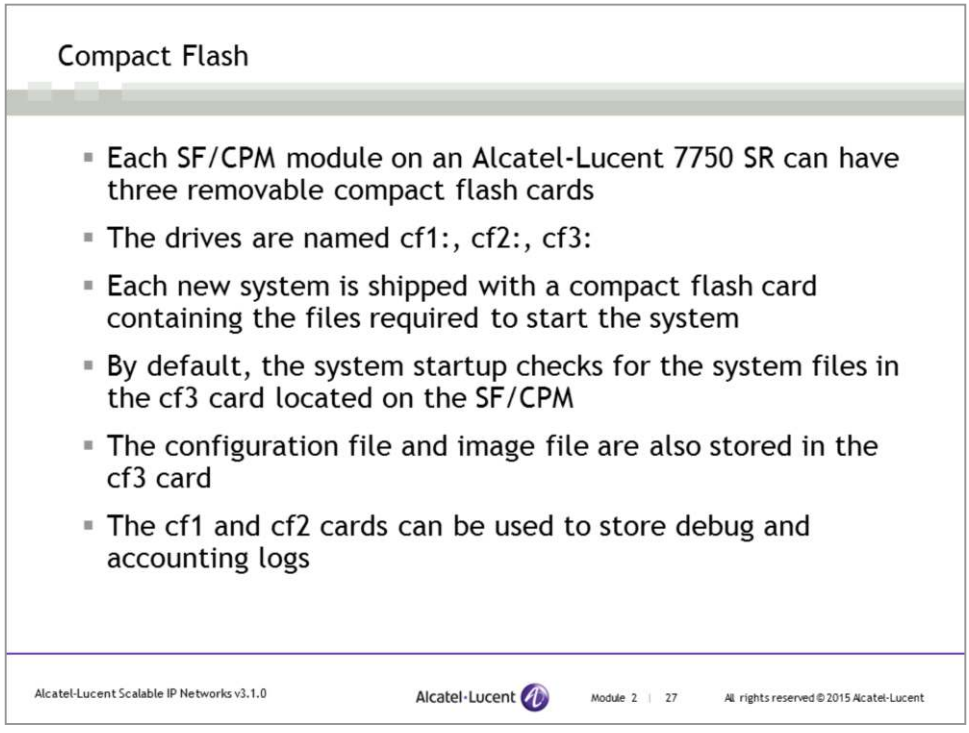
After successful completion of this section, you will be able to:

- Explain the function of bootup components
- Explain the function of BOF parameters
- Explain how to change and display the BOF configuration

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

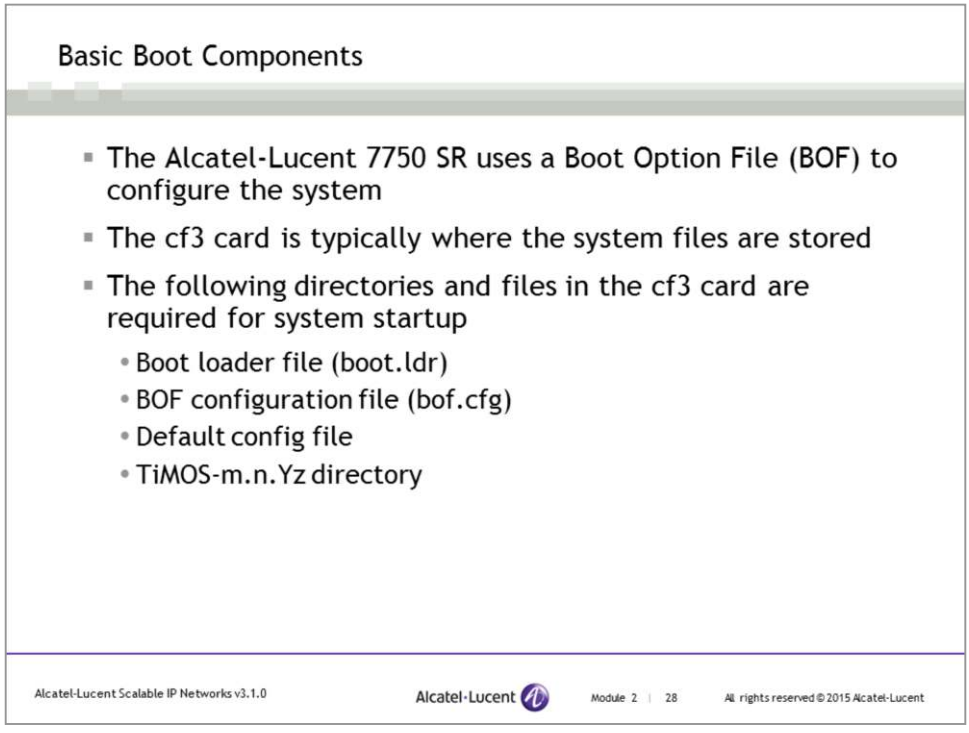
All rights reserved © 2015 Alcatel-Lucent



Each new 7750 SR system is shipped with a compact flash card that contains the files required to start the system. Each SF/CPM module on a 7750 SR can have three removable compact flashes. The drives are named compact flash slot #1 (cf1:), compact flash slot #2 (cf2:), and compact flash #3 (cf3:). The cf3 card is typically where the system files are stored. This is also where the system looks for the files when initializing. Cf1 and cf2 cards can be used to store debug and accounting logs.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Basic operating system

SR products use a Boot Option File (BOF) to configure the system. Each new system is shipped with a Compact Flash (CF) card that contains the files required to start the system.

The cf3 card contains the following directories and files located in the root directory:

boot.ldr - This file contains the system bootstrap image.

bof.cfg - This file contains user configurable information such as:

- Management port IP address
- Location of the image files (primary, secondary, and tertiary)
- Location of the configuration files (primary, secondary, and tertiary)

config.cfg - This default configuration file is very basic, providing just enough information to make the system operational. You can create other configuration files and direct the system to them.

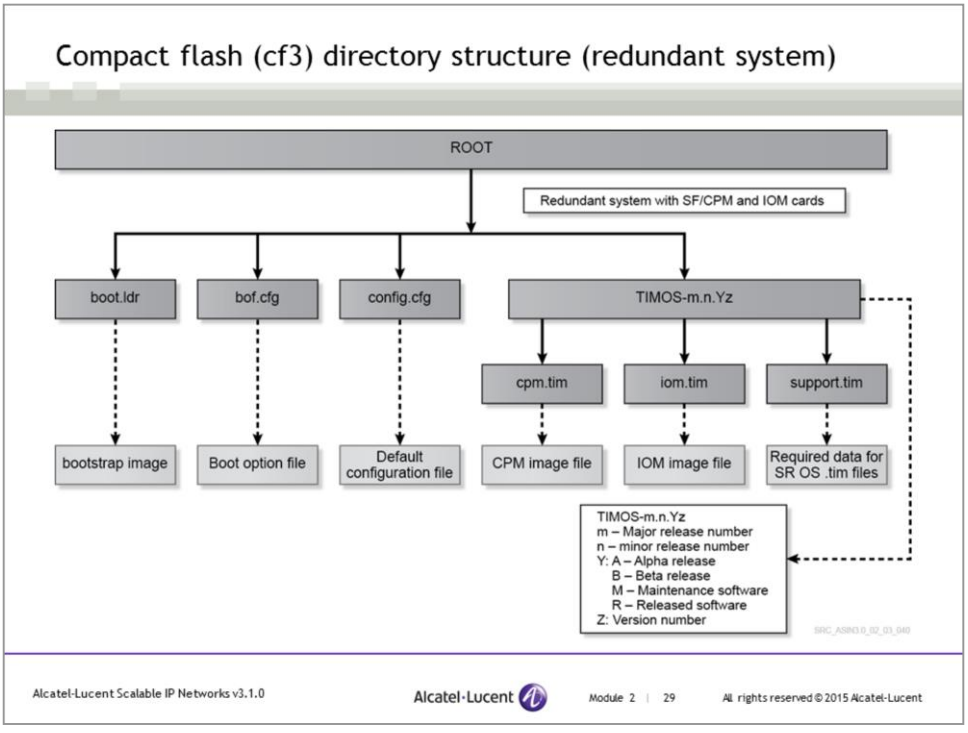
TiMOS-m.n.Yz - This directory is named according to the major and minor software release, type of release and version. For example, if the software release is Version 13.0.R5 of a released software version, the directory name would be: TiMOS-13.0.R5.

For redundant systems with separate SF/CPM and IOM cards, this directory contains three files, cpm.tim, iom.tim, and support.tim.

For non-redundant systems with integrated fabric/control and I/O, there are only two files, both.tim and support.tim.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

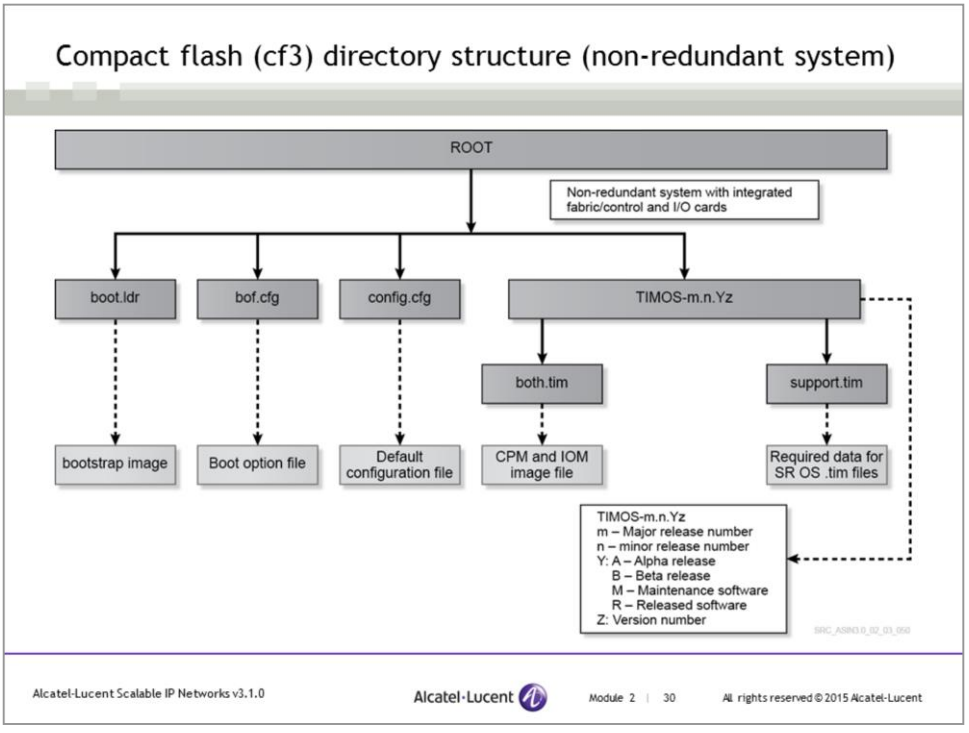


This slide shows the cf3 directory structure and filenames for a redundant system with SF/CPM and IOM cards.

On redundant systems such as 7750 SR-12e, 7750 SR-12, and 7750 SR-7, 7750 SR-e the TIMOS-m.n.Yz directory contains three files, cpm.tim, iom.tim, and support.tim. The cpm.tim file is used for SF/CPM card and the iom.tim file is used for IOM card. The support.tim file contains required data for SR OS .tim files.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

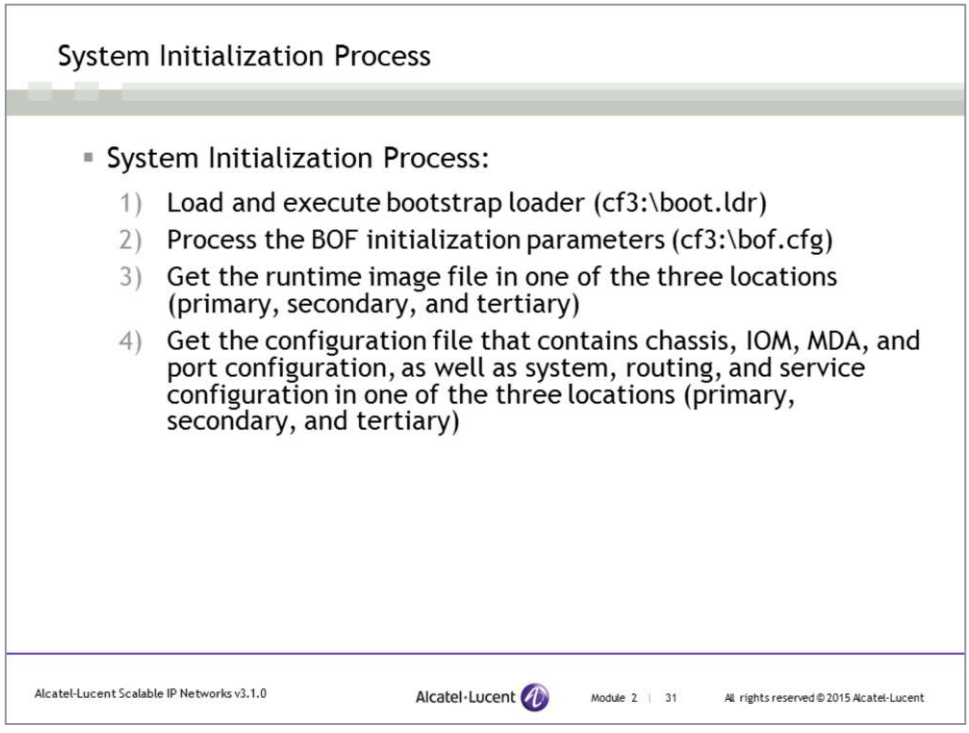


This slide shows the cf3 directory structure and filenames for the fixed form system with integrated fabric/control and I/O cards.

On a non-redundant system such as 7750 SR-c4, the TIMOS-m.n.Yz directory contains only two files. The both.tim file is used for integrated CPM and IOM cards. The support.tim file contains required data for SR OS .tim files.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



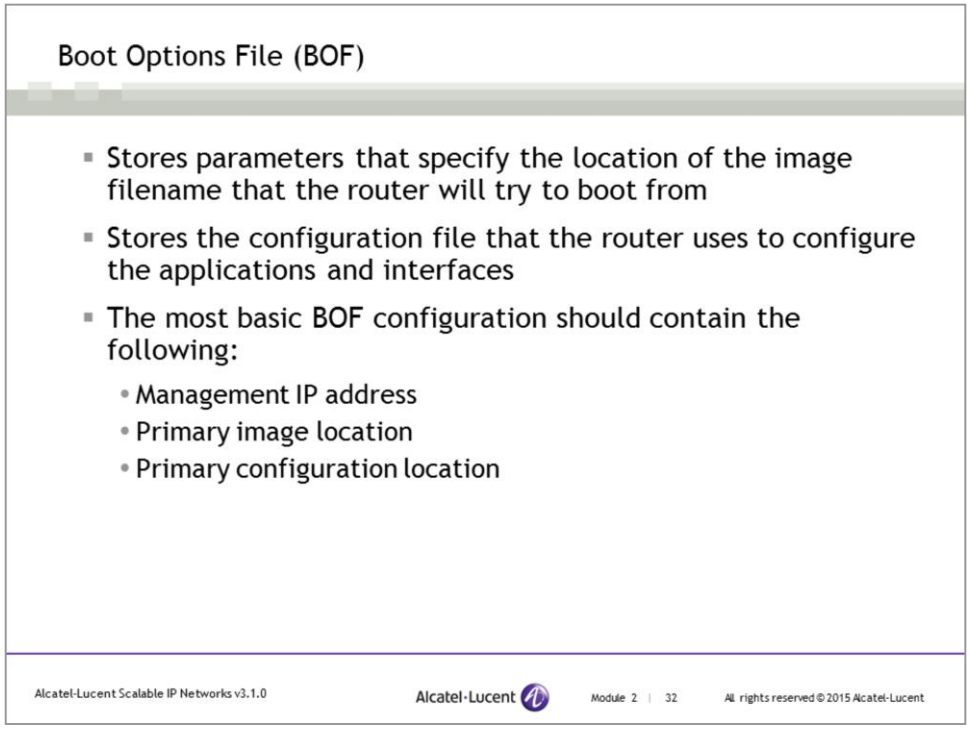
System initialization begins by running the boot.ldr file, which reads the bof.cfg files, waits briefly for any user intervention to halt the boot process, and then begins to load the system image file. If the system image file cannot be loaded, the initialization process fails.

Once the system image is loaded, the system loads the configuration options found in the bof.cfg file. The system then consults the bof.cfg file, which will point to the locations of the runtime image file and the configuration file. The default name for the configuration file is config.cfg. Similar to the runtime image file, up to three locations can be configured for the system to search for the configuration file. The locations can be local or remote. The first location searched is the primary location. If not found, the secondary location is searched. Lastly, the tertiary location is searched.

The configuration file contains chassis, IOM, MDA, and port configuration, as well as system, routing, and service configuration. If the configuration file cannot be found, the system will continue to boot, and a blank configuration will be used.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The Boot Options File (BOF) stores parameters that specify:

- the location of the image filename that the router will try to boot from
- the configuration file that the router uses to configure the applications and interfaces

The most basic BOF configuration should have the following information:

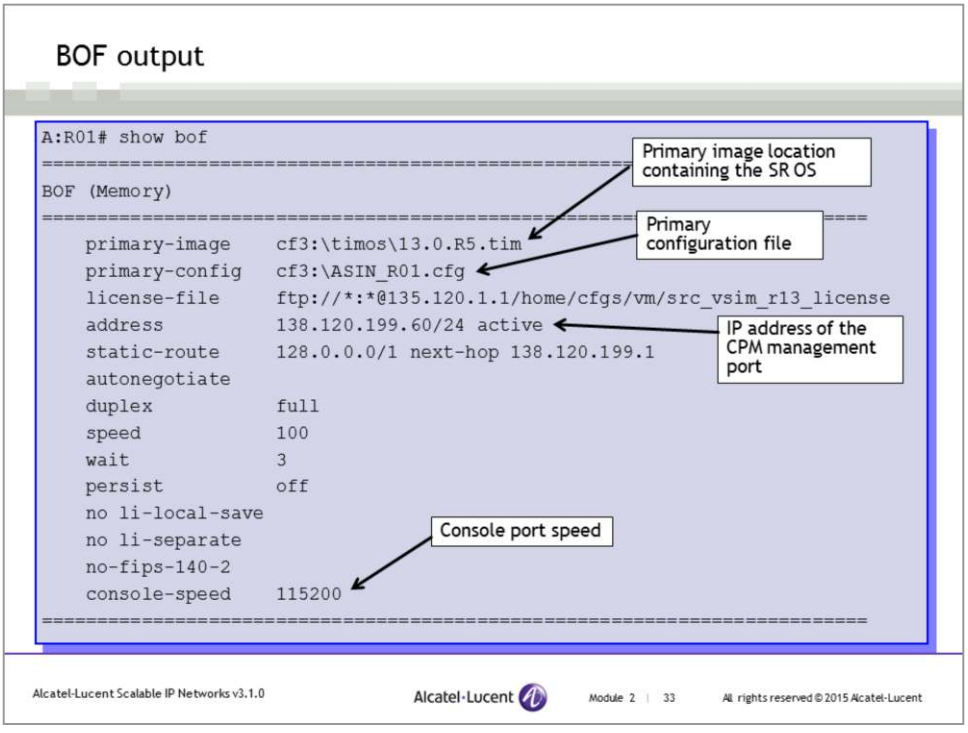
- Management IP address
- Primary image location
- Primary configuration location

The BOF file performs the following tasks:

1. Sets up the CPM Ethernet port (speed, duplex, auto)
2. Creates an IP address for the CPM/Ethernet port
3. Creates a static route for the CPM/Ethernet port
4. Sets the console port speed
5. Configures the Domain Name System (DNS) and DNS servers
6. Configures the primary, secondary, tertiary configuration source
7. Configures the primary, secondary, tertiary image source
8. Configures persistence requirements

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



The slide shows the information contained in the BOF. The primary image location is one of the most important items in the BOF. If the router cannot find an image, router will remain in the boot cycle indefinitely.

Besides the name and location of the image file, the BOF also contains the name and location of the configuration file.

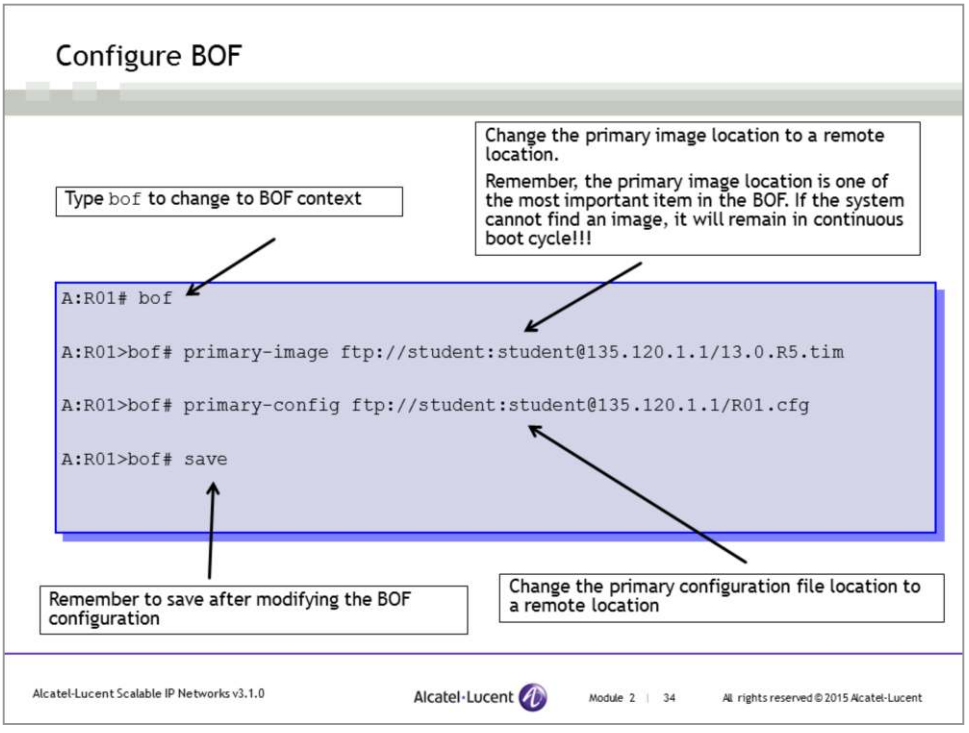
In this slide, the primary image file and configuration file are located in cf3, which is the default location. When the router reboots, it first executes the image file on the cf3 card to boot the operating system. Then, it goes to the cf3 card to get the configuration specified in the BOF, and loads the configuration on the router.

In addition, after the primary configuration location has been defined, when the operator enters the admin save command, the current configuration is saved to the primary configuration file on the cf3 card.

The address referred to in the show bof output is the address of the management port on the Control Processor Module (CPM). The console speed is the default speed of the RS-232 port on the CPM. This speed can be changed in the BOF, but this is rarely necessary.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



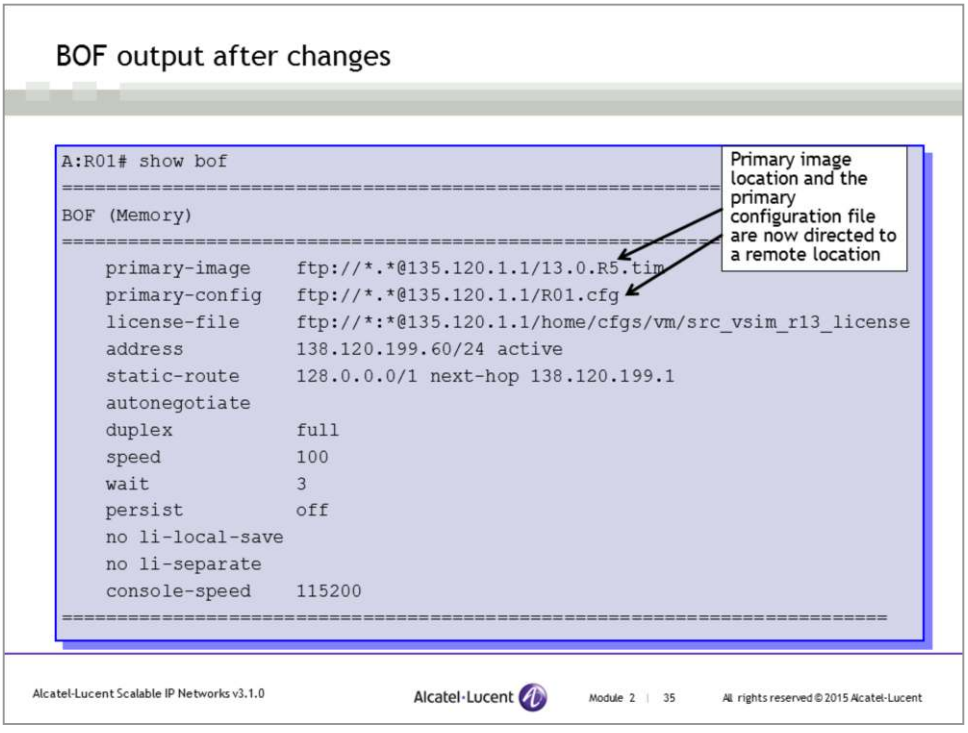
The BOF configuration is done through the BOF command-line interface (CLI) context. CLI is discussed in more details in the next section.

This slide shows some basic `bof` commands. Note that the command-line prompt adds the **>bof** string when you are in BOF context.

After modifying the BOF configuration, execute a save command to save the changes. Otherwise, changes are lost if the system is powered down or the router is rebooted.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

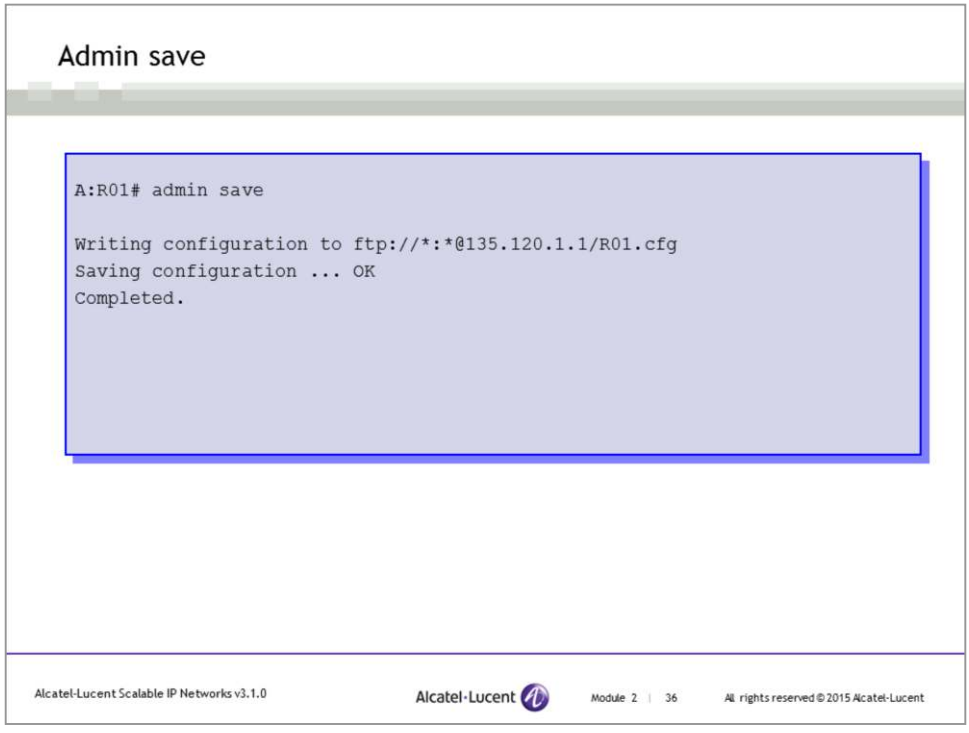


After the BOF primary image location and primary configuration file are modified, the system checks for the primary image location from a remote location (135.120.1.1). Note that the ftp address and the ftp username/password are hidden in the BOF output.

Once the primary image is found, the system then checks for the primary configuration file named R01.cfg from a remote location 135.120.1.1

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In addition, after the primary configuration location has been defined, every time the operator inputs the command admin save, the current configuration is saved to the primary configuration file location as indicated in the BOF. The primary configuration file location as indicated in the last slide, is in the remote location with the specific IP address 135.120.1.1.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

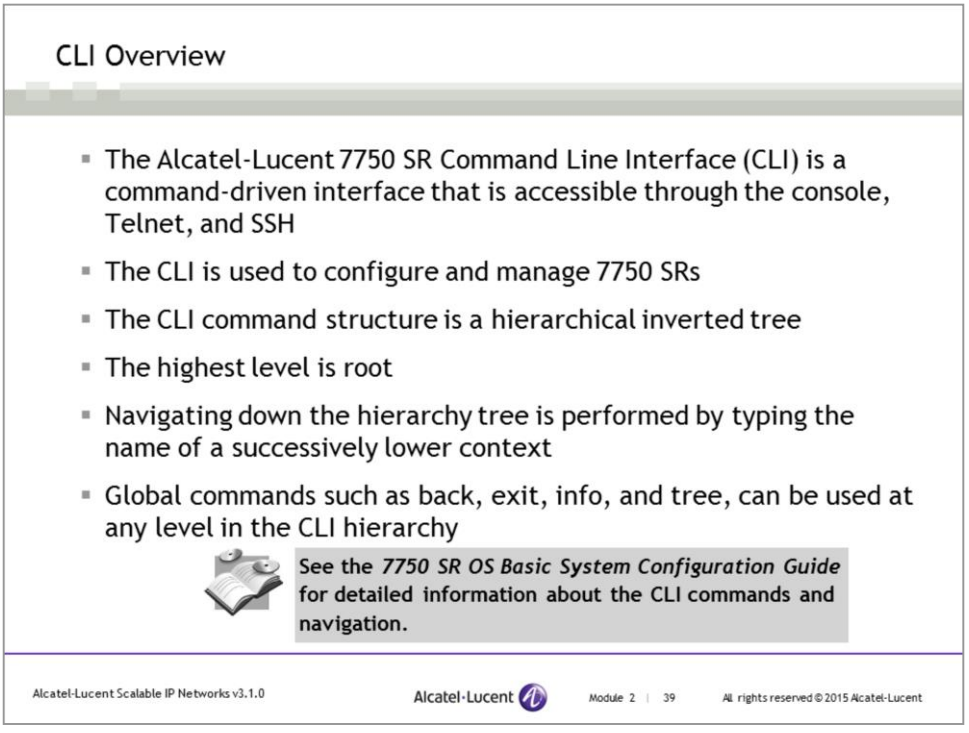
After successful completion of this section, you will be able to:

- Explain the purpose of the Command-Line Interface (CLI)
- Display the CLI command hierarchy
- Describe basic CLI operation and commands

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent



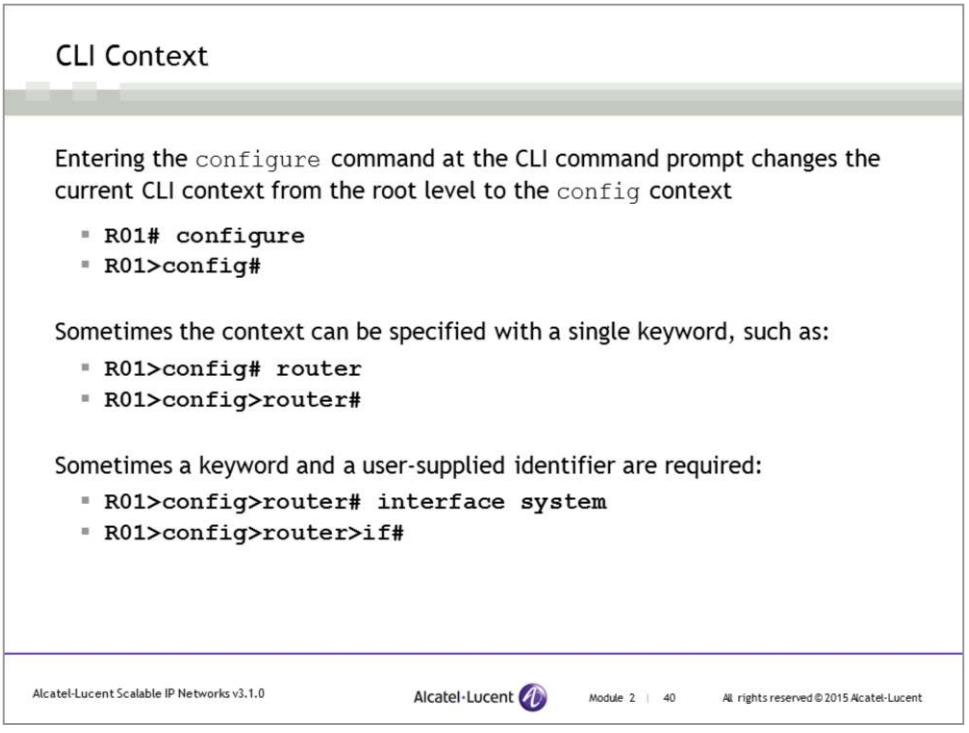
7750 SR Command Line Interface (CLI) is a command-driven interface accessible through the console, Telnet, and Secure Shell (SSH). The CLI can be used for the configuration and management of the 7750 SR.

The CLI command tree is a hierarchical inverted tree. At the highest level is root. Below root are other levels with the major command groups, such as the configure command and the show command. Typing the configure command at the root level navigates down to the configure context. Typing the show command at the root level navigates down to the show context. The active context displays in the command prompt.

Global context commands, such as back, exit, info, and tree, can be entered at any level in the CLI hierarchy.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



At the command prompt (#), entering the **configure** command will change the current CLI context to the **config** context. The active context is displayed in the command prompt.

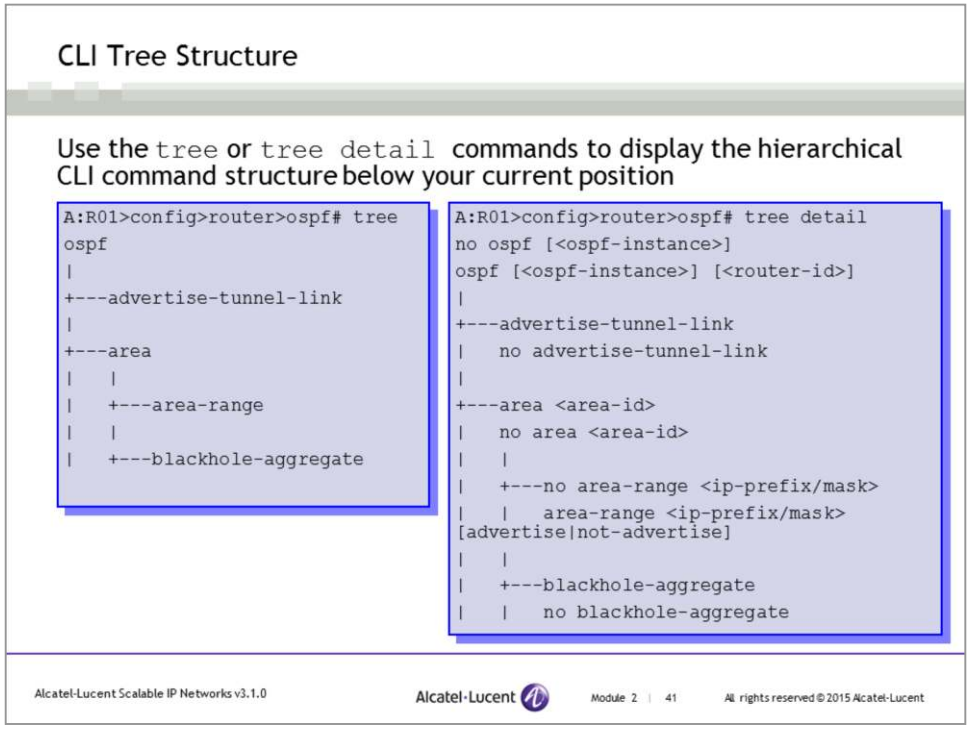
Sometimes, the context you wish to navigate to can be specified in a specific context with a single keyword. For example, when a single keyword, **router**, is entered at the **config** context, the context is changed to the **router** context.

Sometimes a keyword and a user-supplied identifier are required. For example, both a keyword **interface** and a user-supplied identifier **system** are required to change to an **interface** context. Otherwise, CLI returns an error message that a parameter is missing.

```
*A:R01>config>router# interface
                      ^
Error: Missing parameter
*A:R01>config>router#
```

 All rights reserved © 2015 Alcatel-Lucent

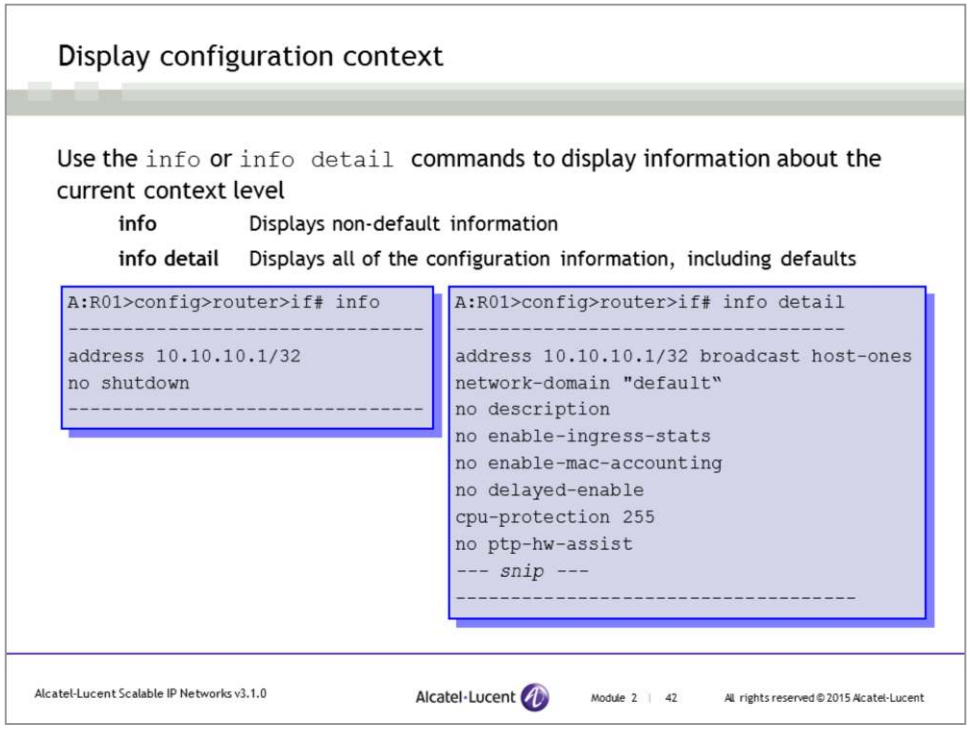
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The **tree** and **tree detail** system commands are help commands. These are useful when searching for a command in a lower-level context.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

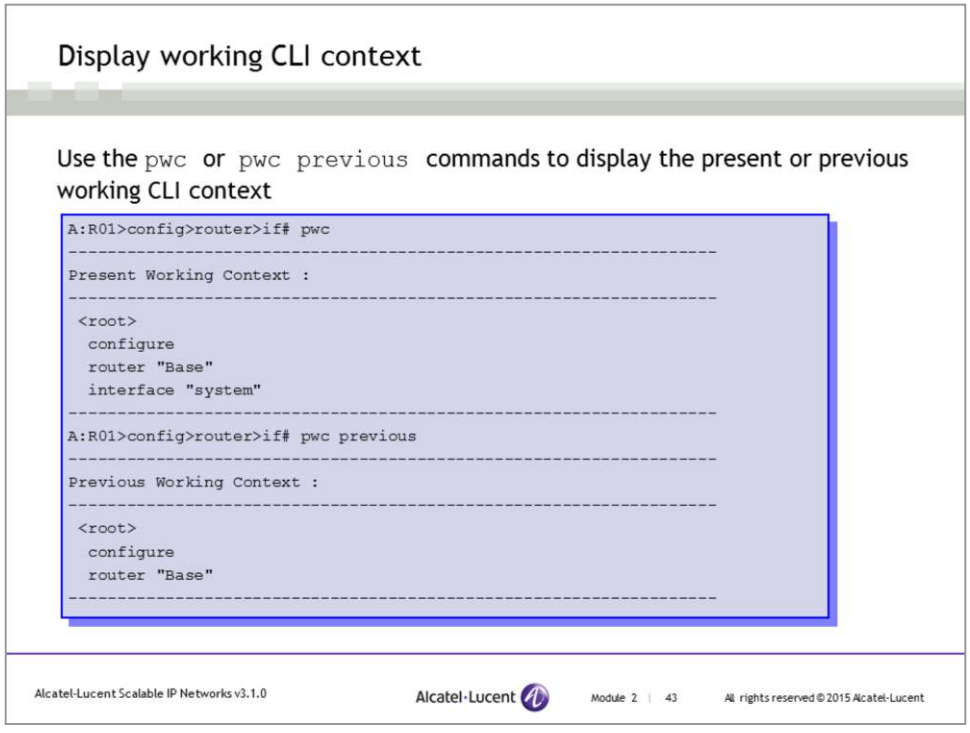
 All rights reserved © 2015 Alcatel-Lucent



Use the **info** and **info detail** commands to display information about the current context level. The **info** command displays non-default information. The **info** detail command displays all configuration information, including defaults.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

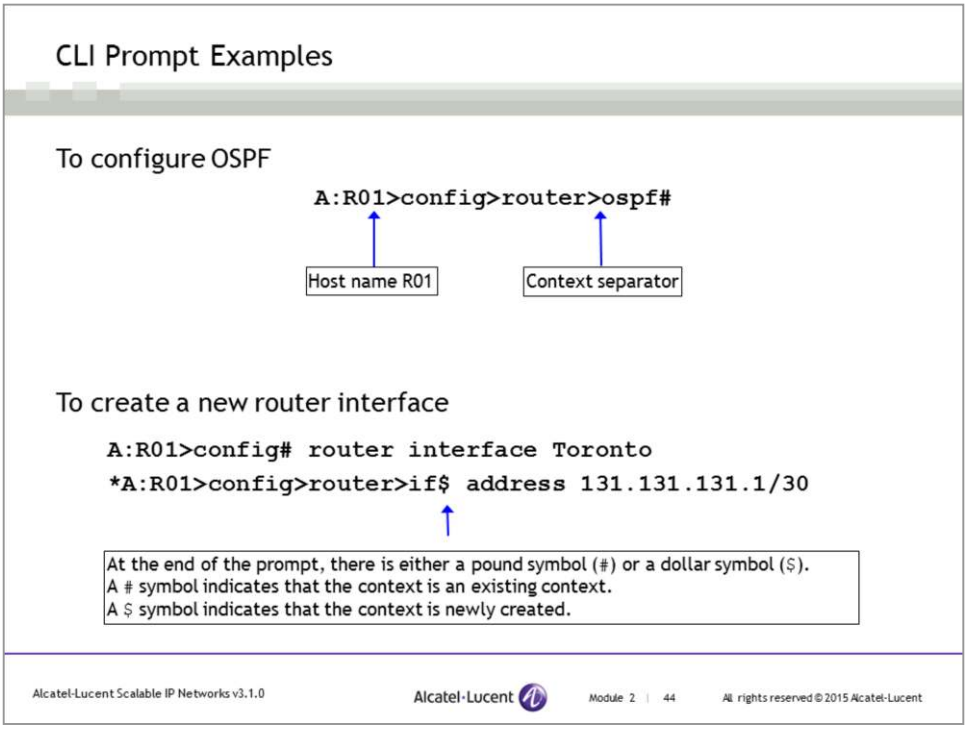
 All rights reserved © 2015 Alcatel-Lucent



Use the **pwc** command to display the current or previous working CLI context. When the keyword **previous** is specified, the previous context is displayed. This is the context entered by the CLI parser upon execution of the **exit** command. The current CLI context is not changed after executing the **pwc** command.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



By default, the CLI command prompt indicates the router being accessed and the current CLI context.

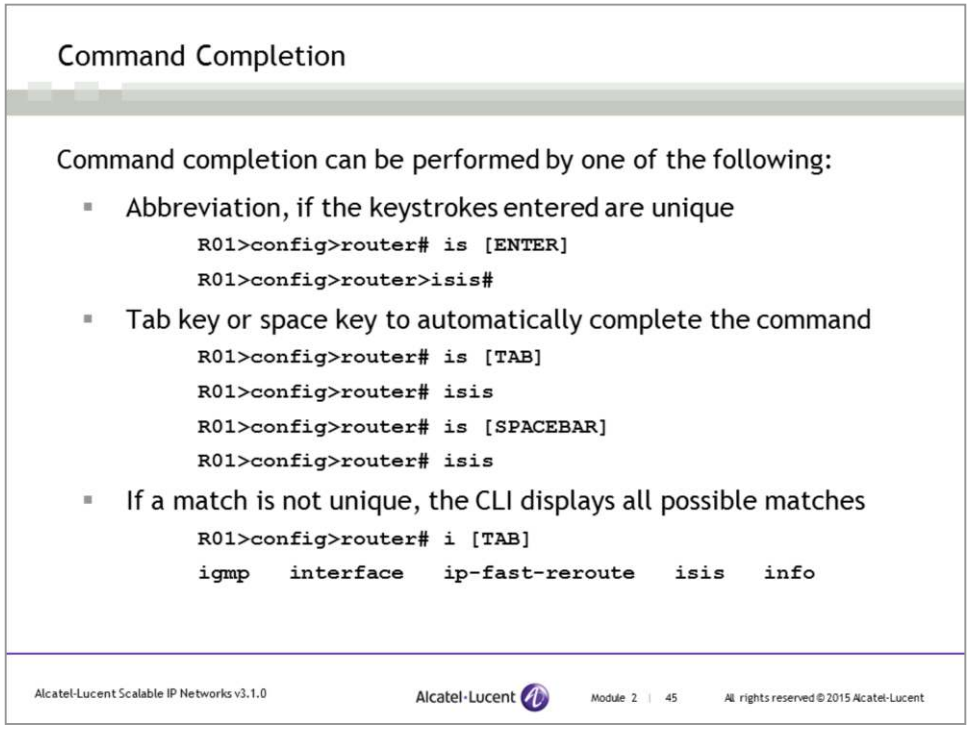
The prompt **`A:R01>config>router>ospf`** indicates the active CLI context. The user is on a router with hostname R01 in the **config>router>ospf** context. In the prompt, the "**>**" symbol is used as a separator between contexts.

At the end of the prompt, there is either a pound sign ("**#**") or a dollar sign ("**$**"). A "**#**" at the end of the prompt indicates the context is an existing context. A "**$**" at the end of the prompt indicates that the context has been newly created.

When changes are made to the configuration file, a "*****" appears at the beginning of the prompt to indicate that changes have not been saved. When an **admin save** command is executed, the "*****" disappears.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

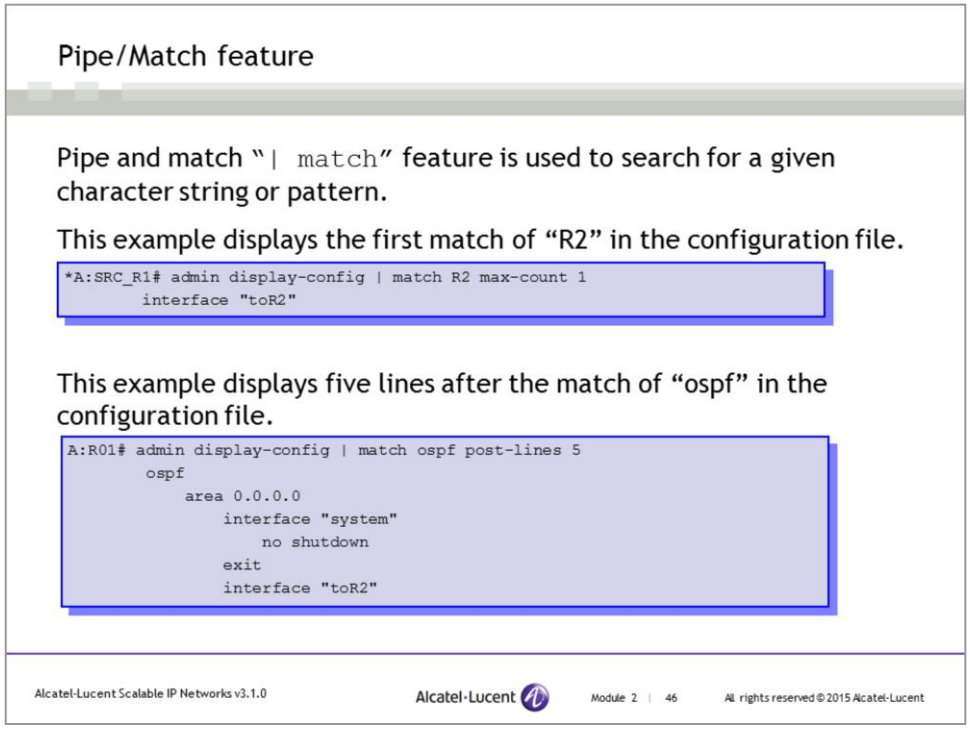


The CLI supports both command abbreviation and command completion.

If the keystrokes entered are enough to match a valid command, the command will be completed automatically. Alternately, the [TAB] key or [SPACEBAR] will display commands matching the letter entered to automatically complete the command. If a match is not found, the CLI displays all possible matches.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

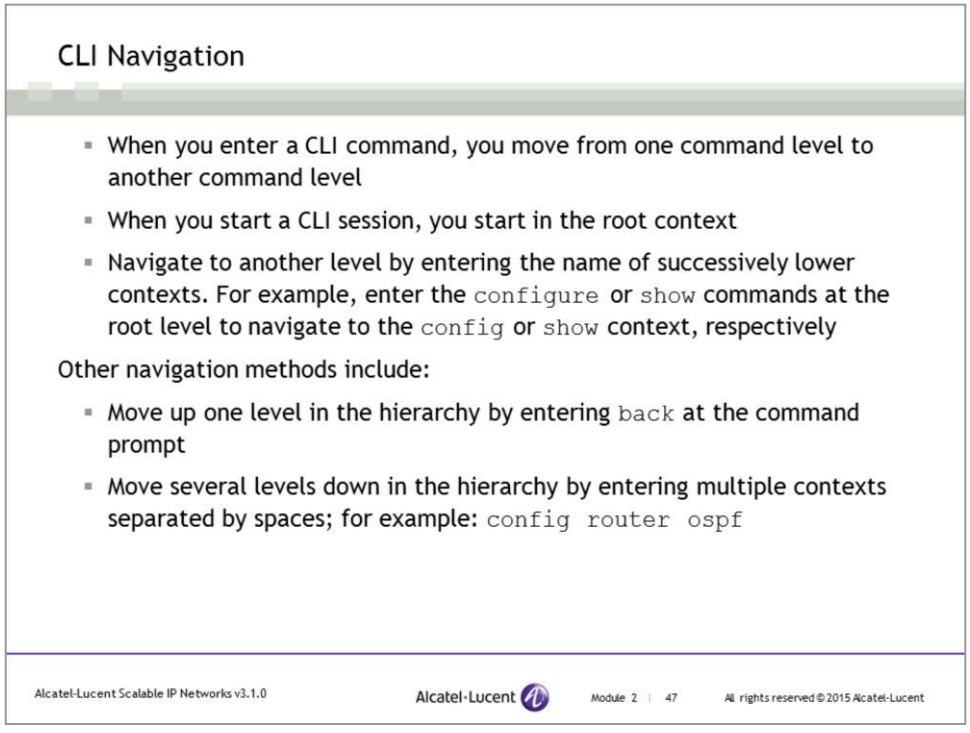
 All rights reserved © 2015 Alcatel-Lucent



A pipe/match **(| match)** feature is very useful, especially if you need to find information from a large amount of CLI command output.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



When initially entering a CLI session, you are in the ROOT context. Navigate to another level by entering the name of the successively lower contexts.

In a given CLI context, enter a command to navigate to a lower context level. It is also possible to navigate multiple contexts by entering a list of commands separated by spaces.

The following example shows two methods to navigate to a router interface level:

Method 1:

*A:R01# configure

*A:R01>config# router

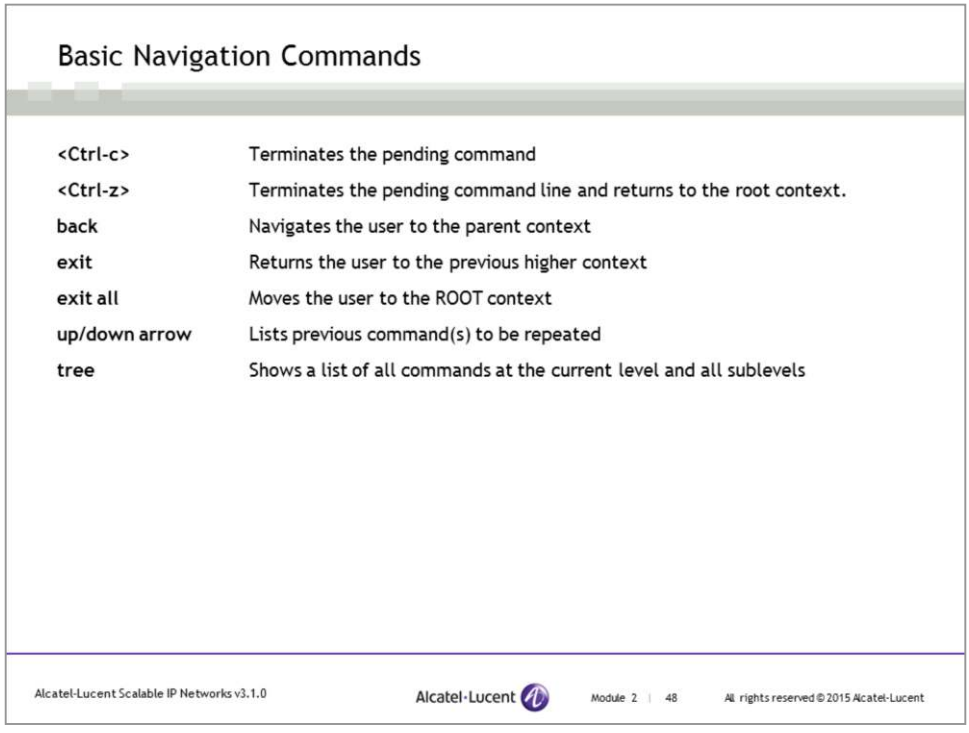
*A:R01>config>router# interface Toronto

Method 2:

*A:R01# configure router interface Toronto

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

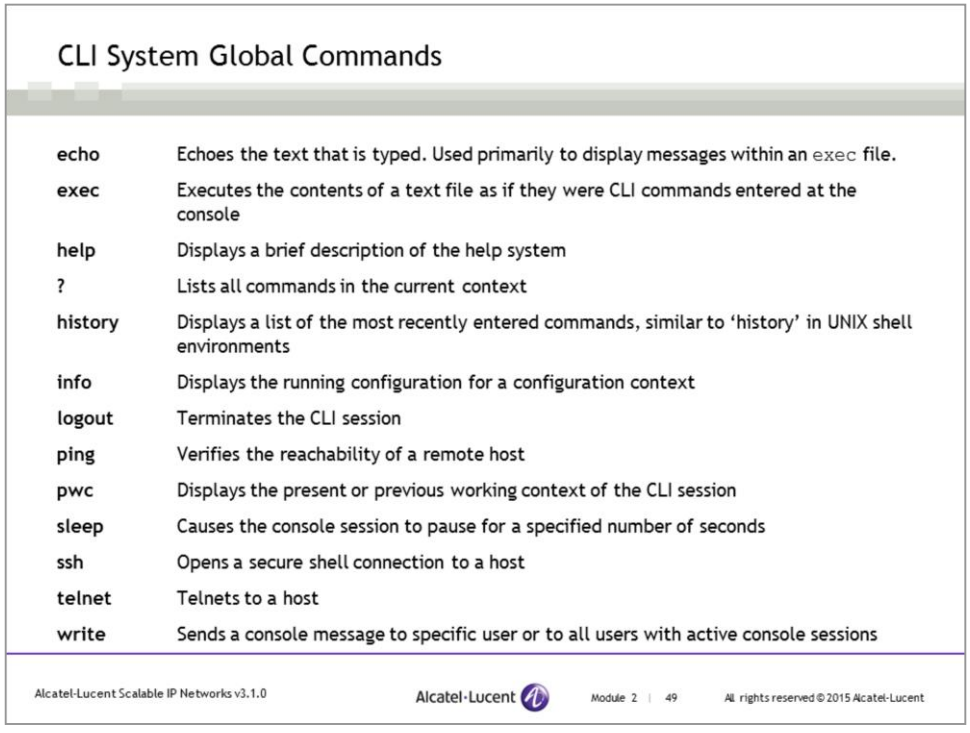


Console control commands are used to navigate in a CLI session and to display information about a console session. Many of these commands are global commands, which means that the commands can be executed at any level of the CLI hierarchy. These commands are used to move up or down in the command hierarchy or to exit from a particular CLI command level.

This slide shows some of the more commonly used navigation commands.

 All rights reserved © 2015 Alcatel-Lucent

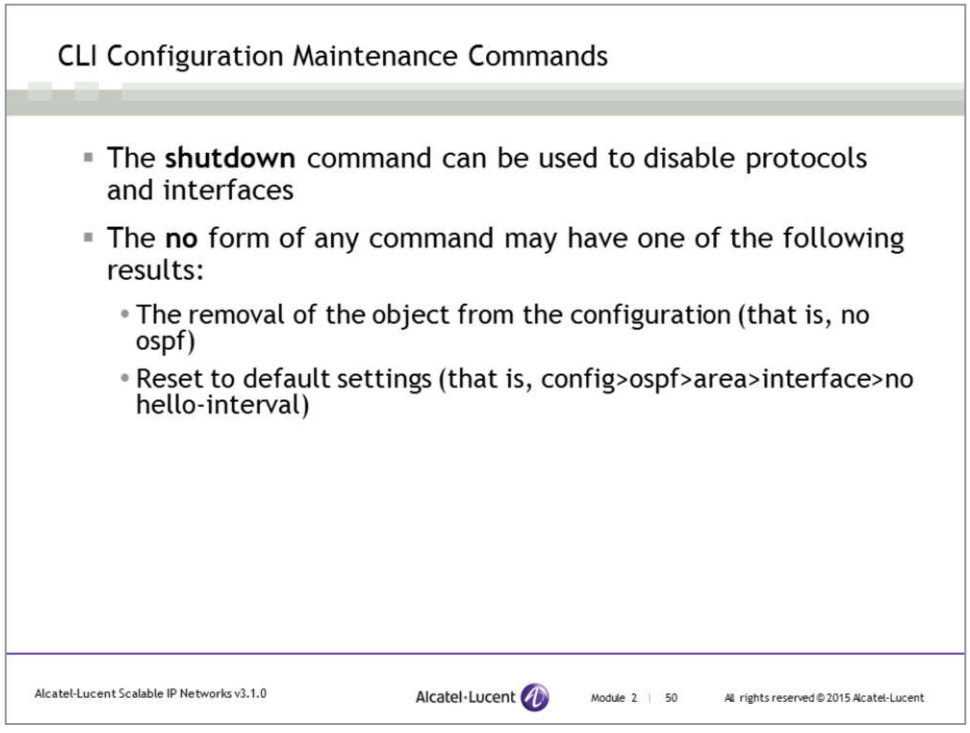
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows a list of some global system commands. Enter **help globals** in the CLI to see a list of all global system commands. Global commands can be executed from anywhere in the CLI hierarchy.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



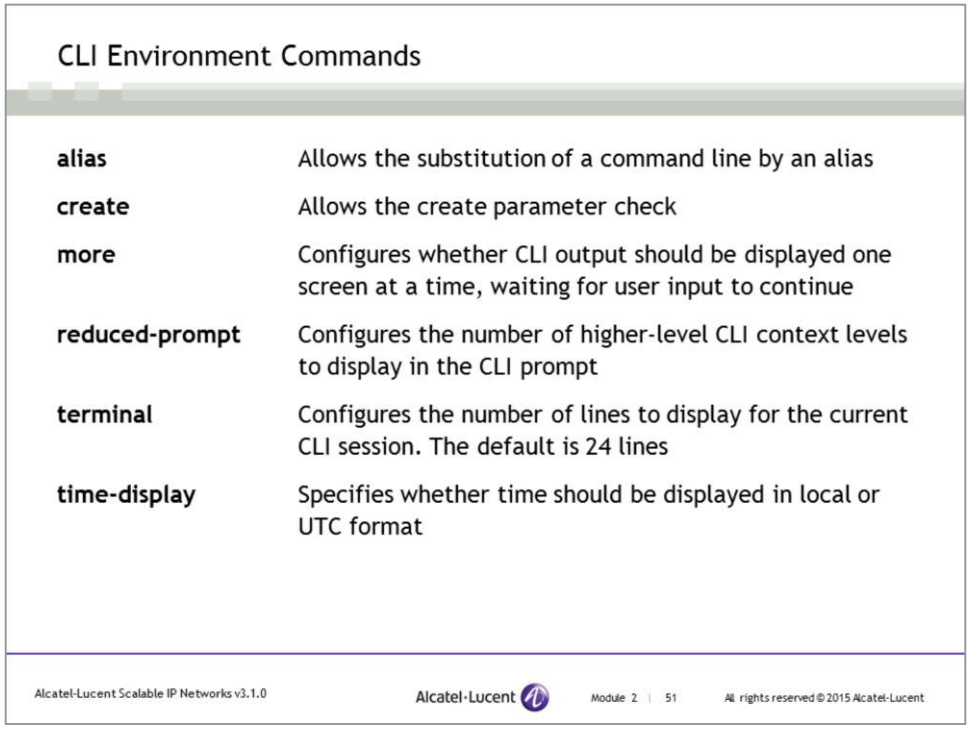
There are two other special commands that deserve particular attention: **shutdown** command and **no** command.

- The **shutdown** command is used to disable protocols and interfaces. This command is necessary to disable objects before they can be deleted. Once the command is applied to an object, it is saved in the configuration file. This command does not change, reset, or remove any configuration settings or statistics. By default, many levels are operationally shutdown and need to be **no shutdown** to be operational.
- The **no** form of any command is used to remove commands that have been previously applied. For example, all ports on the 7750 SR are shut down by default when the system is first powered on and must be enabled with the **no shutdown** command.

To restore the settings after issuing a **no** command, you must reconfigure the router by re-entering the command you removed, rebooting from a configuration file that has correct configuration, or doing an exec command on a configuration file that contains the correct settings.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

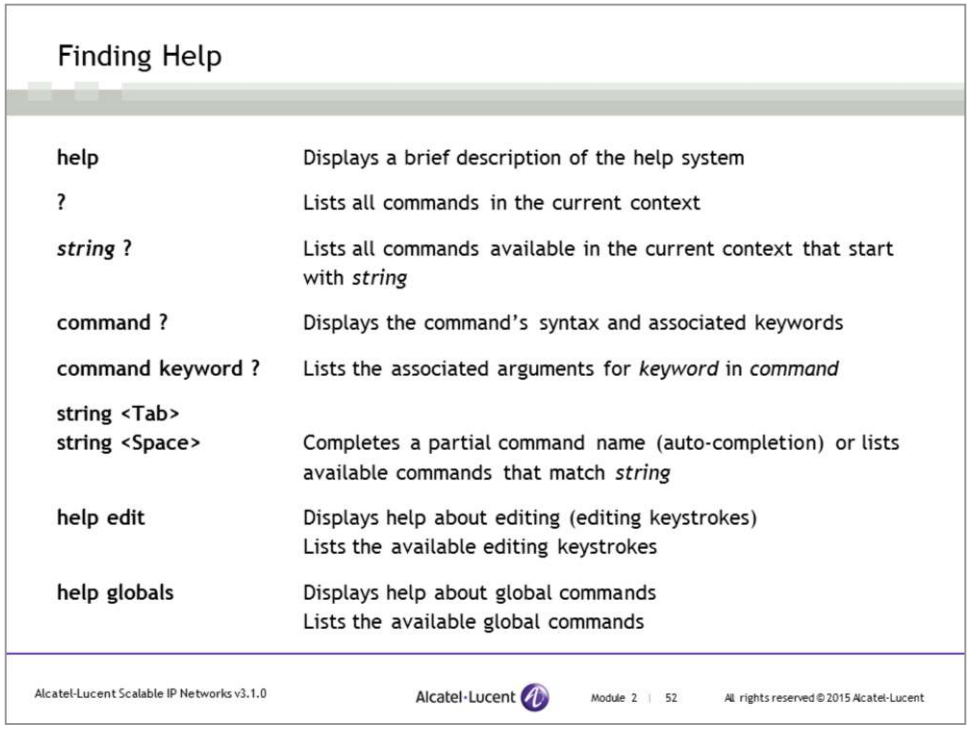


CLI environment commands are used to customize session preferences for a CLI session.

This slide displays some useful commands to control the environment of the 7750 SR, such as the appearance of the prompt and the number of lines on the terminal screen.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

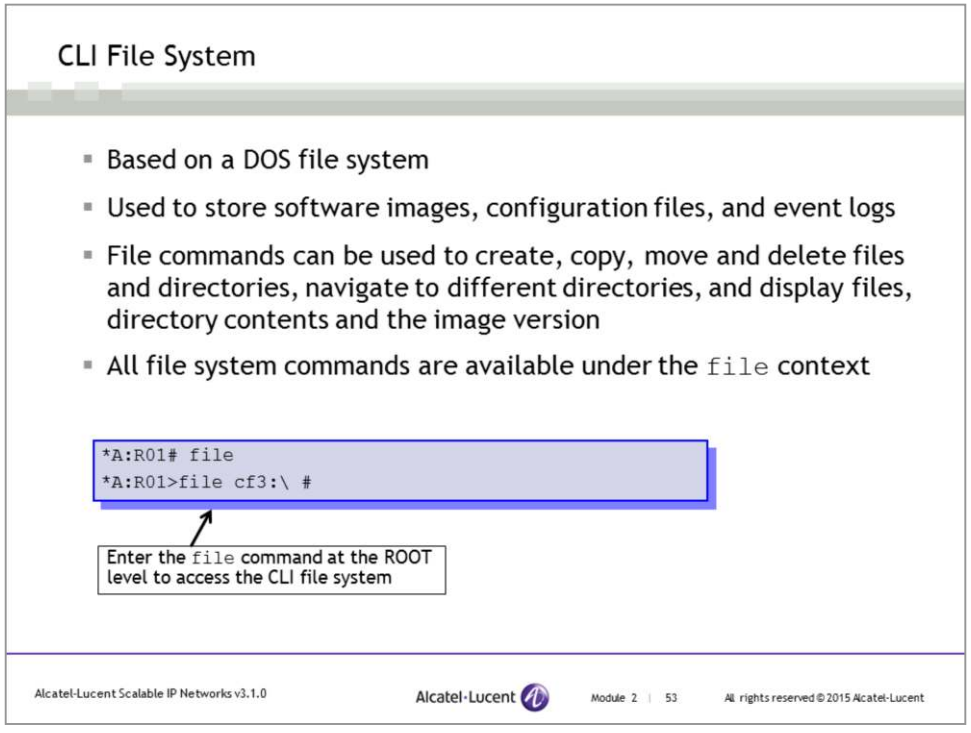
 All rights reserved © 2015 Alcatel-Lucent



The **tree** and **tree detail** system commands are also help commands that are useful when you search for a command in a lower-level context.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



The SR OS file system is used to store files used and generated by the system (for example, image files, configuration files, logging files and accounting files).

The file commands can be used to copy, create, move, and delete files and directories, to navigate to a different directory, or to display file or directory contents and the image version.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

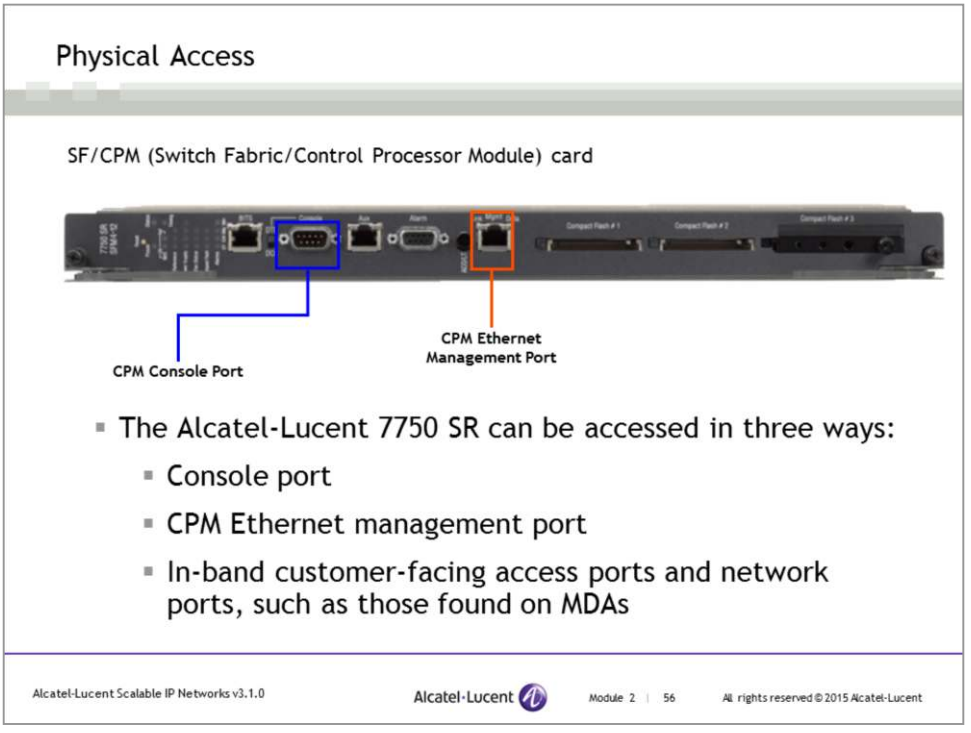
After successful completion of this section, you will be able to:

- List different ways to access the Alcatel-Lucent 7750 SR
- Identify basic steps to configure a system from startup
- Configure and verify the operation of IOM and MDA
- Describe the functions of event logs and provide a list of possible log sources and log destinations
- Configure an event log and display the contents of the log
- Describe the purpose of default logs and the special use log

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 2 | 55 All rights reserved © 2015 Alcatel-Lucent



The 7750 SR can be accessed in three ways:

Console port — A DB-9 serial port, which is enabled by default. The default settings are:

Baud Rate: 115 200
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None

CPM Ethernet Management port — A 10/100 Ethernet management port for out-of-band Management

In-band ports — Access ports and network ports on MDAs for in-band Management

In-band Management

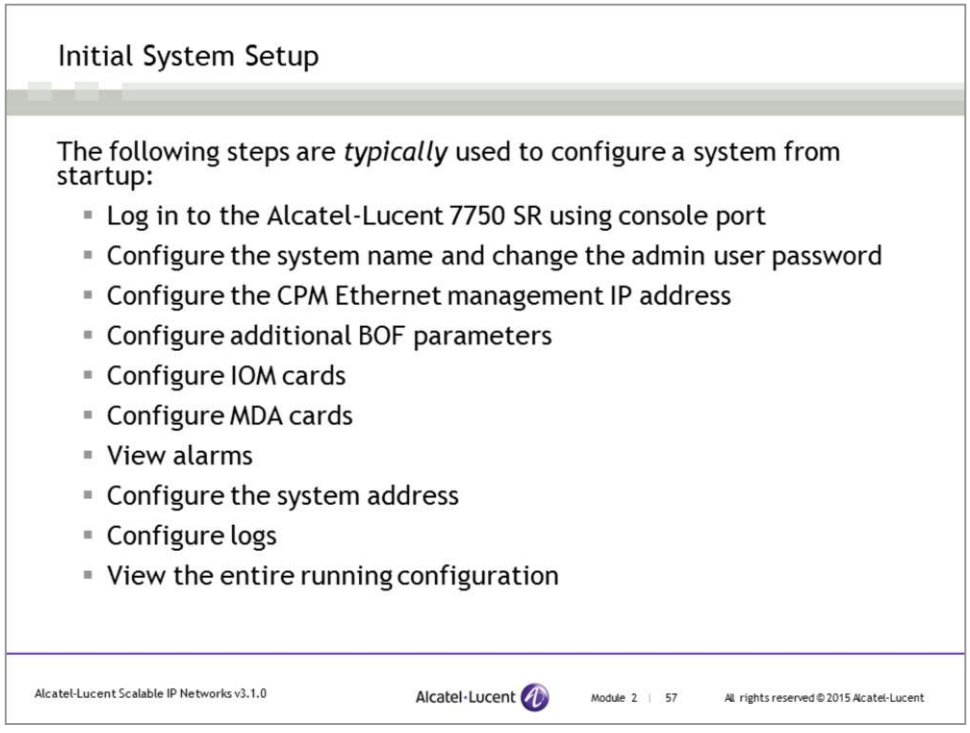
In-band management shares the same path traversed by the data plane. It is easy to setup and involves management sessions to one of the router's IP interfaces using an active physical port on the device.

Out-of-band Management

Out-of-band management uses a dedicated path to access the router. The management path is different than the data path.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

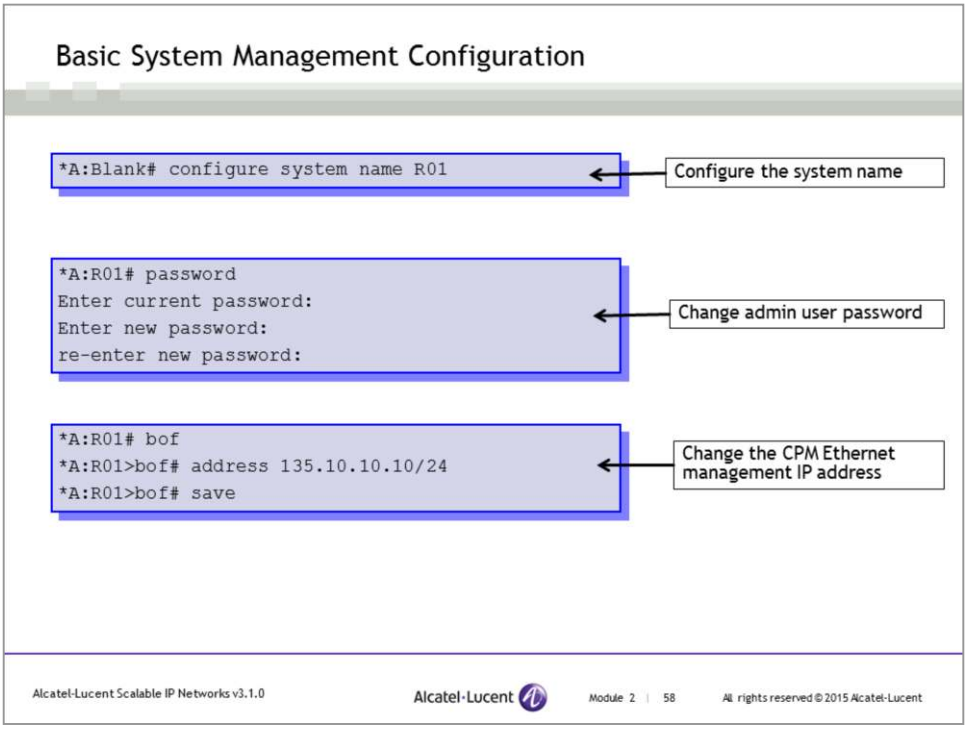


There are many steps that are typically used to configure a system from startup. Not all of these steps will necessarily be followed for every system, but you can use this series of steps as a template for what is *typical* for initial setups.

Note that these steps are an example to configure a 7750 SR that contains both IOM and MDA.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



Some basic configuration on the 7750 SR is usually required before you place the router in service:

- System name
- Admin password
- CPM Ethernet management port IP address
- IOMs, MDAs, and ports

System Name - Any ASCII printable string up to 32 characters. The system name is configured in the config CLI context. If the name contains spaces, the name must be enclosed in quotation marks to delimit the start and end of the name. The system name becomes part of the CLI prompt.

Passwords - The default login and password is admin. This password should be changed before your router is placed in service.

The system automatically creates at least one admin user (the default) and must retain at least one admin user unless you are using an external protocol, such as RADIUS or TACACS+, to provide authentication.

You can configure the following password parameters:

Aging — The maximum number of days (1 to 500) that a password remains valid before the user must change the password. The default is no aging enforced.

Attempts — The number of unsuccessful login attempts that are allowed in a specified time period. If the configured threshold is exceeded, the user is locked out for a specified time. In the following example, a user is locked out for 10 minutes if 4 unsuccessful login attempts occur in a 10-minute period.

Count: 4
Time (minutes): 10
Lockout (minutes): 10

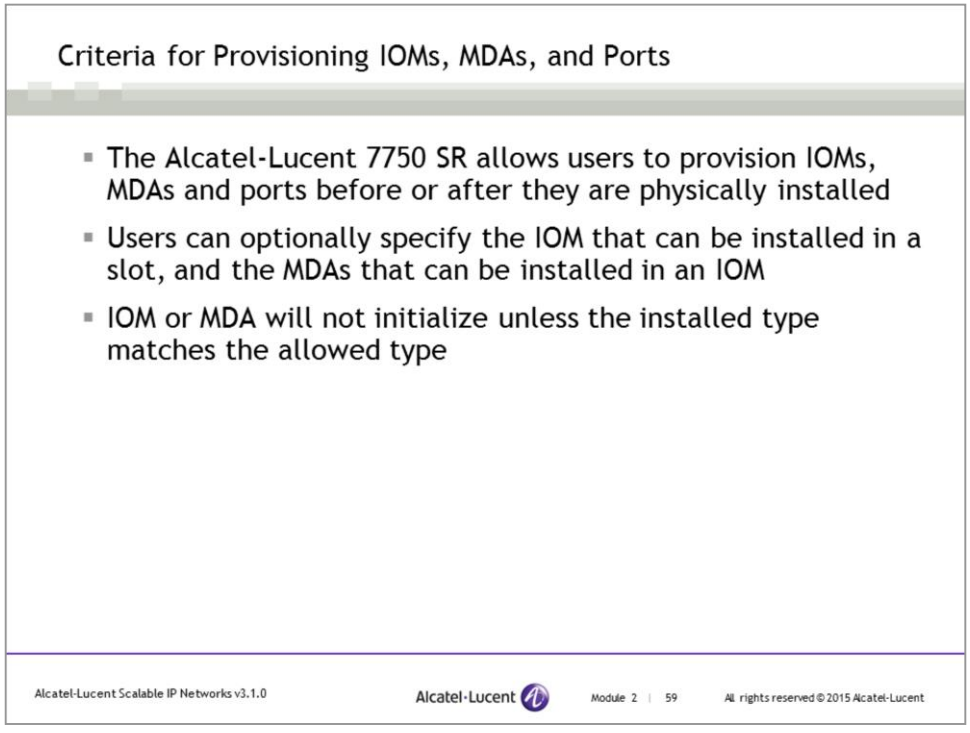
Authentication Order — You can configure the sequence in which password authentication is attempted for the RADIUS, TACACS +, and local methods.

Complexity — You can specify whether passwords must contain uppercase and lowercase characters, special characters, and numerical values.

Minimum Length — You can specify the minimum number of characters (1 to 8) required for a password.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

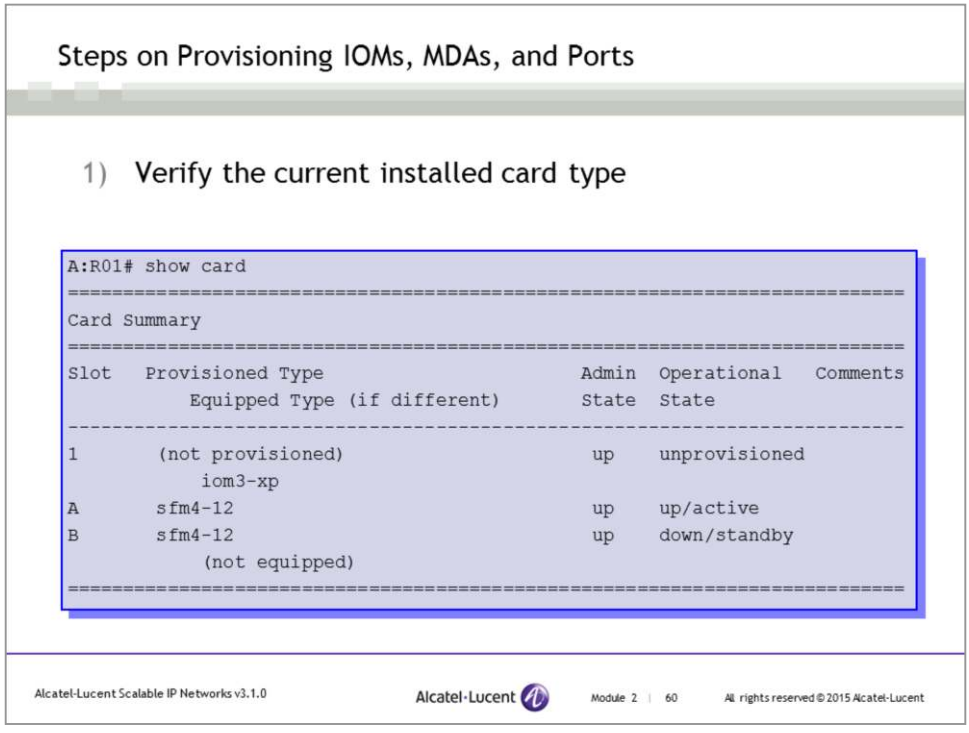


There are a few key points to keep in mind when provisioning the 7750 SR.

1) Users have the ability to provision IOMs, MDAs, and ports before or after they are physically installed.
2) Users can optionally specify which IOMs are permitted to be installed in a particular slot and which MDAs are permitted to be installed in a particular IOM. An IOM or MDA will not initialize unless the installed type matches the permitted type. This feature should be used with caution since it can prevent an IOM or MDA from functioning properly.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



There is a certain order that should be followed when configuring the 7750 SR. The following steps must be performed in the order listed below :

1. Verify the current installed card type
2. Choose a chassis slot and provision the IOM type for the slot.
3. Verify the current installed MDA type
3. Choose an MDA slot and specify the MDA type for the slot.
4. Choose a port and configure the port.

IOMs, MDAs, and ports must be enabled with the **no shutdown** command. All ports are initially shut down when the products are initialized.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Steps on Provisioning IOMs, MDAs, and Ports

2) Select a chassis slot and provision the IOM type for the slot

```
*A:R01# configure card 1
*A:R01>config>card# card-type "iom3-xp"
*A:R01>config>card# no shutdown
```


All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Steps on Provisioning IOMs, MDAs, and Ports

3) Verify the current installed MDA type

```
A:R01# show mda
===============================================================================
MDA Summary
===============================================================================
Slot  Mda    Provisioned Type                        Admin     Operational
               Equipped Type (if different)          State     State
-------------------------------------------------------------------------------
 1     1     (not provisioned)                       up        unprovisioned
              m10-1gb-xp-sfp

===============================================================================
```


All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 2 | 62 All rights reserved © 2015 Alcatel-Lucent

Steps on Provisioning IOMs, MDAs, and Ports

4) Select an MDA slot and specify the MDA type for the slot
5) Select a port and configure it

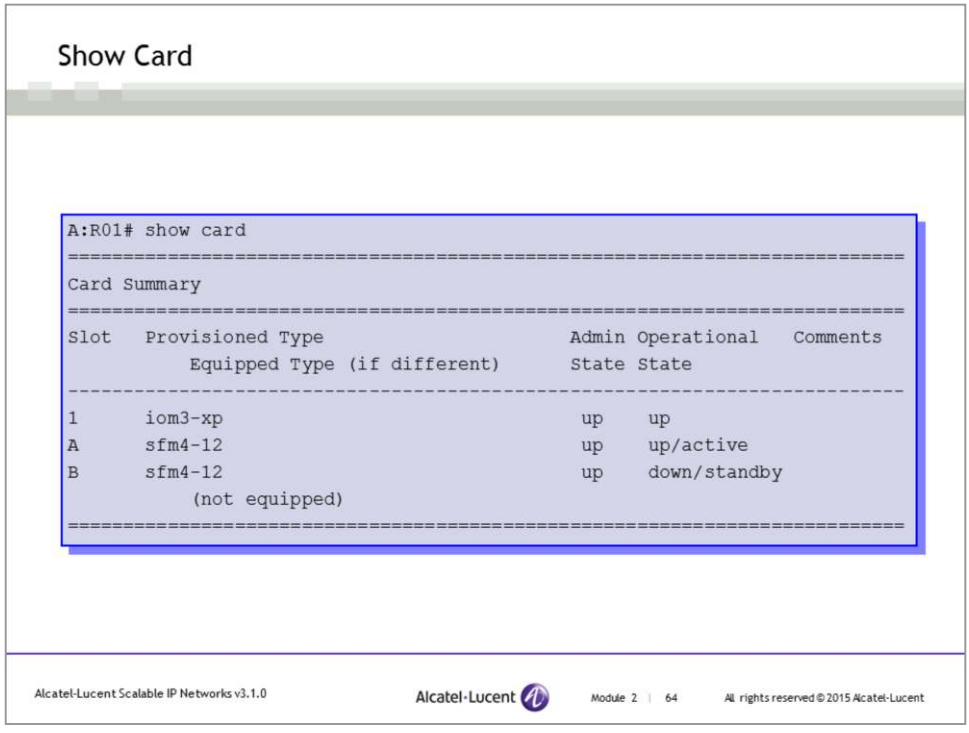
```
*A:R01>config>card# mda 1
*A:R01>config>card>mda# mda-type "m10-1gb-xp-sfp"
*A:R01>config>card>mda# no shutdown

*A:R01# configure port 1/1/1
*A:R01>config>port# no shutdown
```

Step 4: Provision the MDA type for the slot

Step 5: Configure the port

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Once the IOM is configured, it is useful to use the **show card** command to view the IOM types a particular slot is configured for and to give the status of the card (up or down). This command can also be used to determine active and standby CPM (A or B).

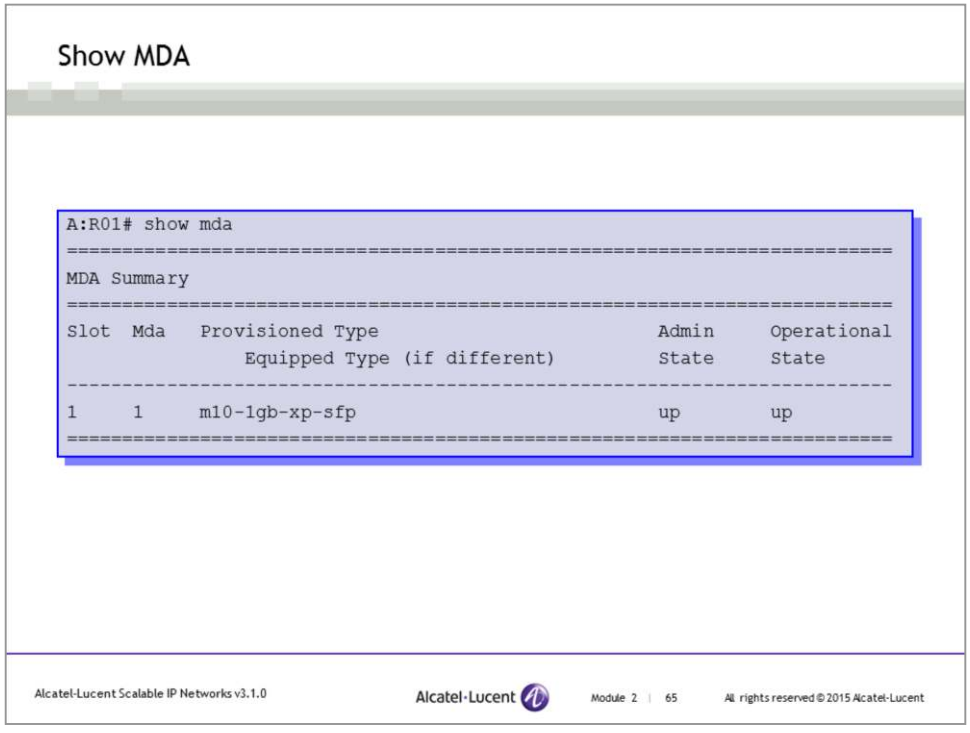
To view the card on slot 1 only, use the **show card 1** command.

To view the card on slot 1 in detail, use the **show card 1 detail** command. The following partial output shows the detailed information about a card on slot 1.

```
A:R01# show card 1 detail
===============================================================================
Card 1
===============================================================================
Slot      Provisioned  Type                        Admin   Operational    Comments
                Equipped Type (if different)       State   State
-------------------------------------------------------------------------------------------------------------------------------
1           iom3-xp                                  up       up

IOM   Card Specific Data
        Capabilities                 : SR
        Clock source                 : none
        Named Pool Mode              : Disabled
        Fail On Error                : Disabled
        Available MDA slots          : 2
        Installed MDAs               : 1
:
:
```

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Similar to the **show card** command, the **show mda** command displays what MDA types a particular MDA is configured to support and the status of the MDA (up or down).

To view a MDA on slot 1/1 only, use the **show mda 1/1** command.

To view a MDA on slot 1/1 in detail, use the **show mda 1/1 detail** command. The following partial output shows the detailed information about a MDA on slot 1/1.

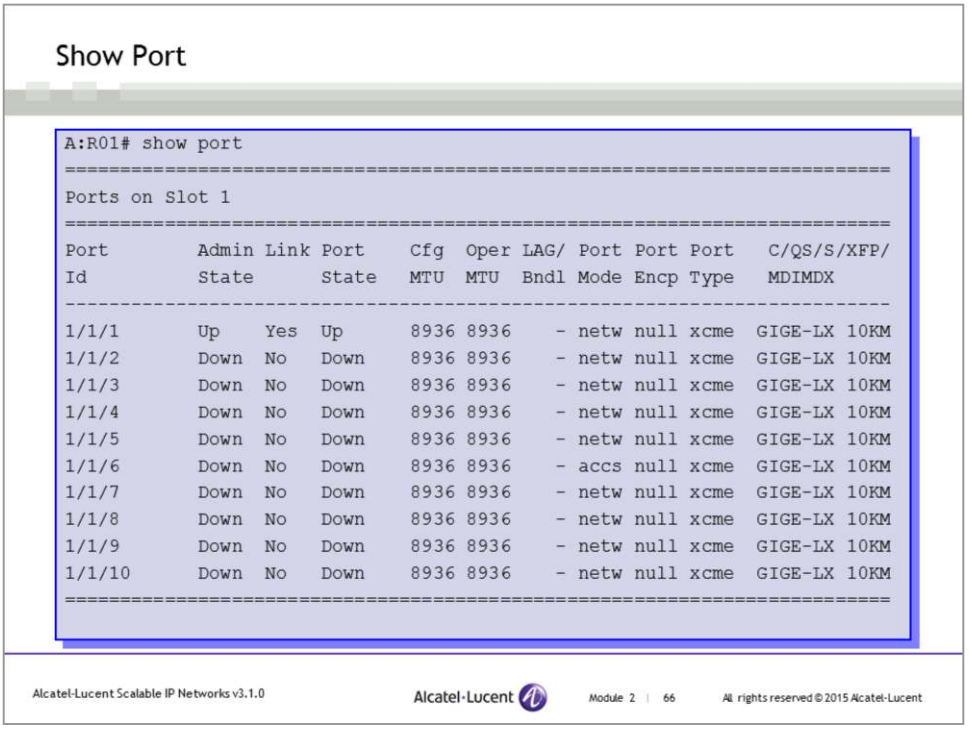
```
A:R01# show mda 1/1 detail
===============================================================================
MDA 1/1 detail
===============================================================================
Slot  Mda  Provisioned Type                        Admin     Operational
                   Equipped Type (if different)    State     State
-------------------------------------------------------------------------------
1     1    m10-1gb-xp-sfp                         up        up

MDA  Specific Data
       Maximum port count              : 10
       Number of ports equipped        : 10
       Network ingress queue policy    : default
       Capabilities                      : Ethernet
       Fail On Error                     : Disabled
       Egress XPL error threshold      : 1000
       Egress XPL error window         : 60
       Ingress XPL error threshold     : 1000
       Ingress XPL error window        : 60
:
```

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

:

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Once the port has been enabled by executing the **no shutdown** command on the port, the **show port** command displays the status, MTU, port mode, port encapsulation, and port type of all ports in the slot. If the port number is specified in the **show port** command, details about the particular port are displayed. Sometimes it is useful to show all ports on one MDA using the command **show port 1/1**.

The following partial output shows the detailed information about port 1/1/1.

A:R01# show port 1/1/1

==========

Ethernet Interface

==========

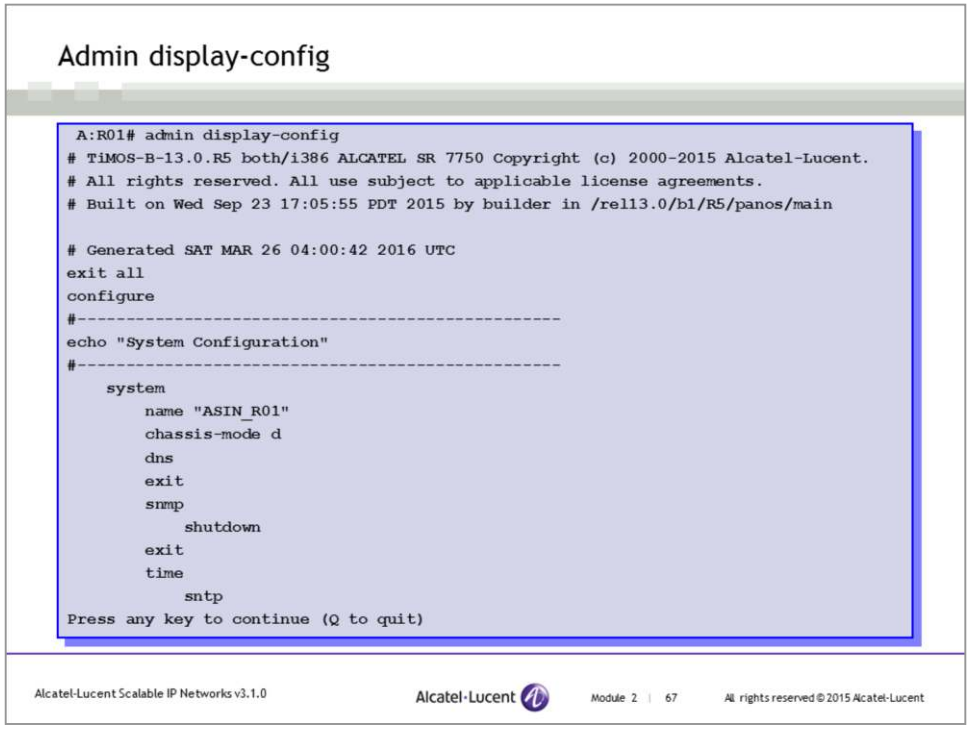
Description	**: 10/100/Gig Ethernet SFP**		
Interface	**: 1/1/1**	**Oper Speed**	**: 1 Gbps**
Link-level	**: Ethernet**	**Config Speed**	**: 1 Gbps**
Admin State	**: up**	**Oper Duplex**	**: full**
Oper State	**: up**	**Config Duplex**	**: full**
Physical Link	**: Yes**	**MTU**	**: 8936**
Single Fiber Mode	**: No**	**Min Frame Length**	**: 64 Bytes**
IfIndex	**: 35684352**	**Hold time up**	**: 0 seconds**
Last State Change	**: 01/26/2016 05:00:14**	**Hold time down**	**: 0 seconds**
Last Cleared Time	**: N/A**	**DDM Events**	**: Enabled**
Phys State Chng Cnt	**: 1**		

:

:

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

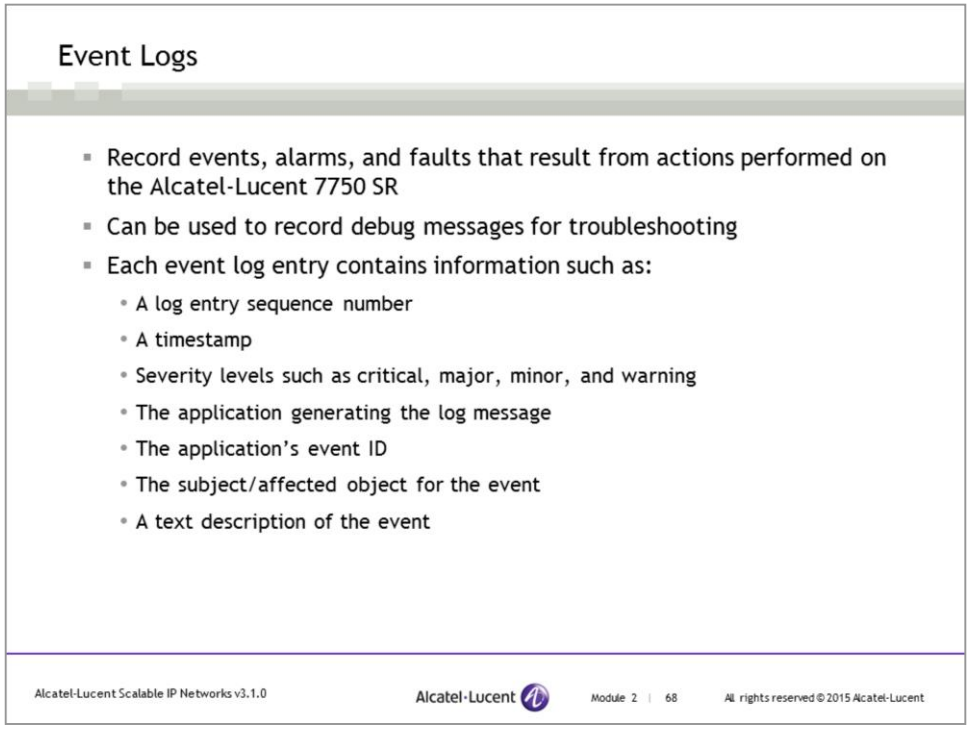


It is often useful to know the current version of the operating system running on a system and its current running configuration. The **admin display-config** command can be used to display this information.

This slide shows a partial output of the **admin display-config** command. The first portion of the output displays the current version of the operating system running on the router. The router then outputs the entire configuration of the router.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

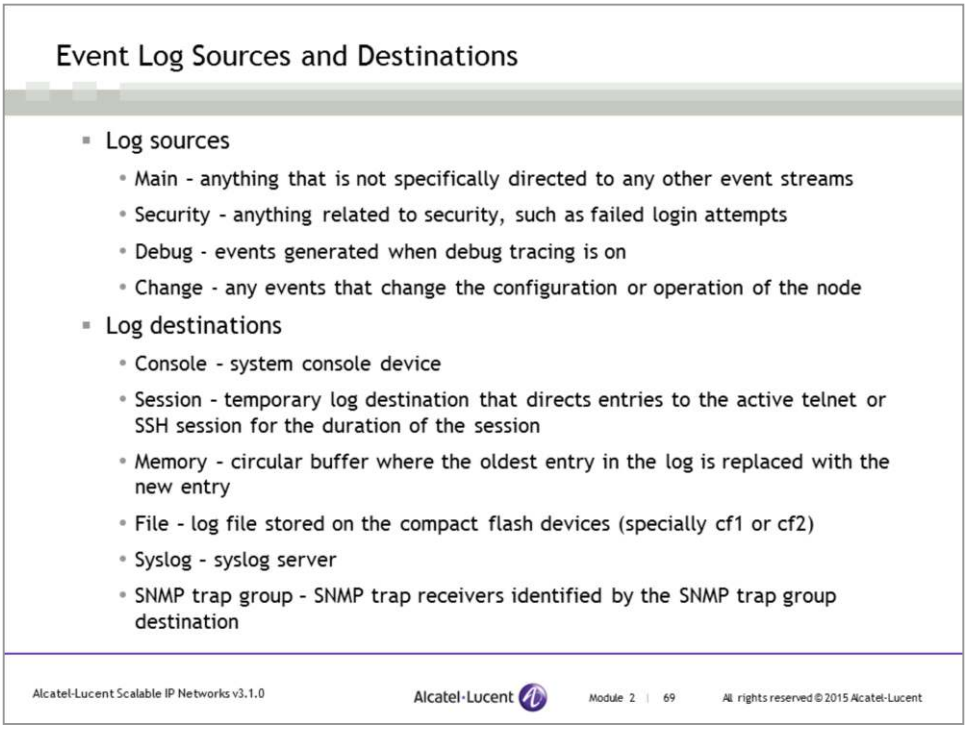


Event Logs

The 7750 SR keeps very extensive logs of events, alarms, traps, and debug/trace messages. The event logs are used to monitor events and troubleshoot faults. You can configure the type of logging information that is captured and where to send the captured logging information.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Log sources

Applications and processes in the 7750 SR generate event logs. The logs are divided into four types or streams of logs:

- Main events – Events not assigned to other event categories/sources
- Security events – Events related to security, such as failed login attempts
- Debug events – Events that contain trace or other debugging information as a result of turning on debug/trace
- Change events – Events that affect the configuration and operation of the node

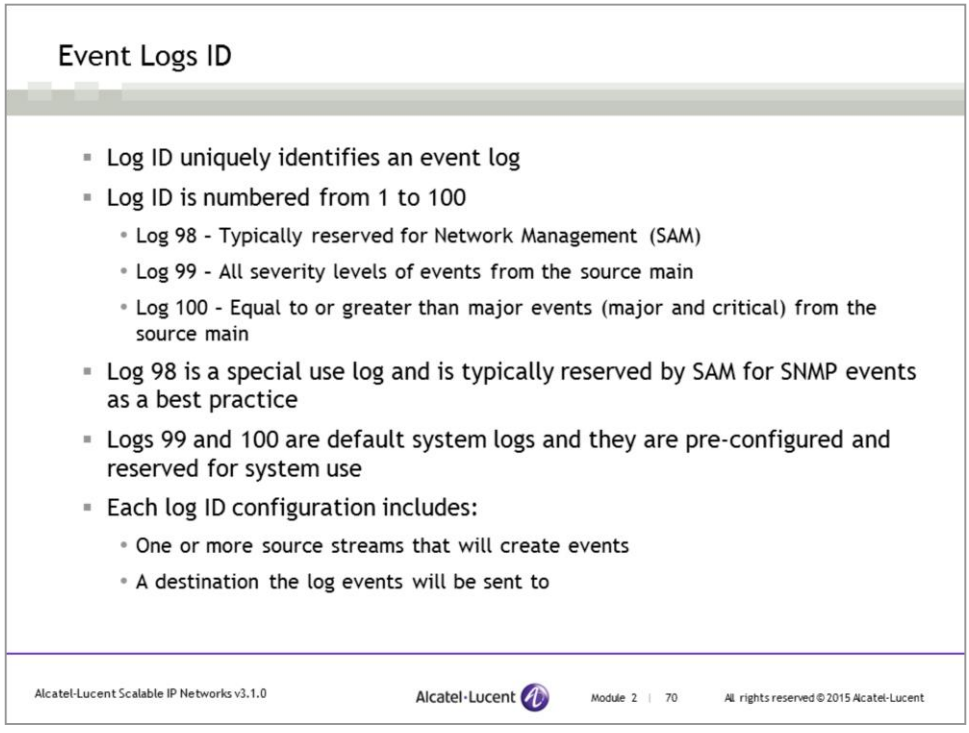
Log destinations

You can configure the destination for the contents of a log-id. A log-id can be directed to one of the following destinations:

- Console – the physical 9-pin console port of the 7750 SR
- Session – a Telnet or SSH session. Sessions are temporary log destinations valid only for the duration of the session. When the session is terminated, for example, when the user logs out, the event log is removed.
- Memory – a circular buffer where the oldest entry is overwritten when the buffer is full
- File – log file that can be used by both event logs and accounting logs. The log file is stored on the compact flash device (specially cf1 or cf2) in the file system. It is recommended that event and accounting logs not be configured on the cf3 device used for software images and bootup configuration
- Syslog – event log information that can be sent to a syslog server
- SNMP trap group – event log information that can be sent to an SNMP trap group. All events and traps are time-stamped and numbered per destination. Traps are numbered sequentially per destination and stored in memory.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



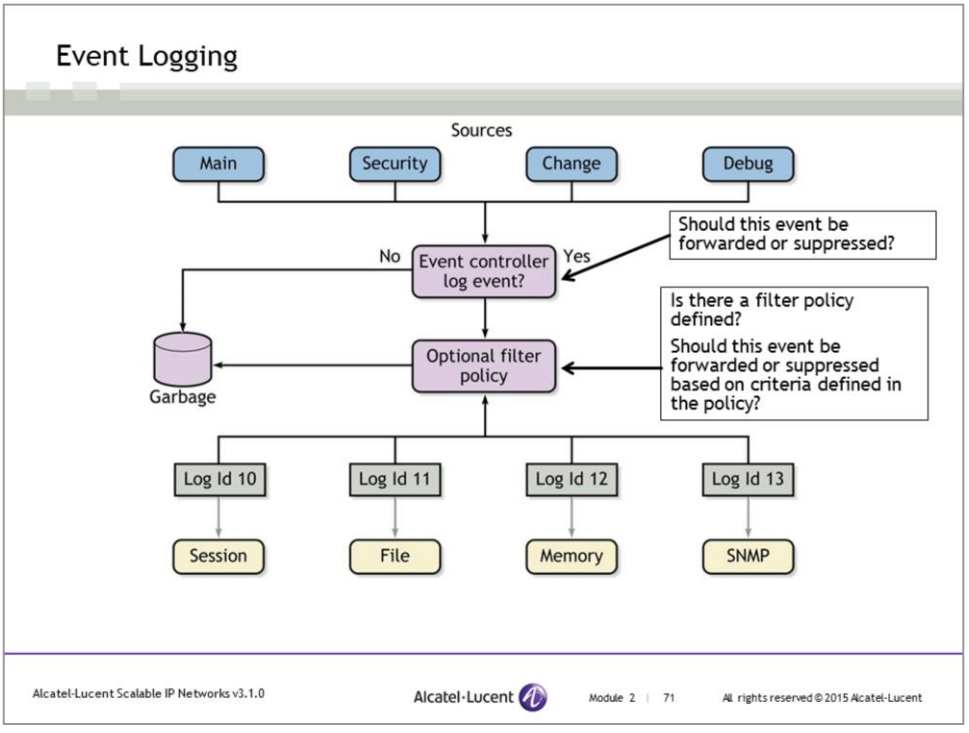
Event Logs ID

Events from any of the four source streams are sent to an event log identified by a unique log identifier (log ID). The configuration of each log ID includes which streams will create events in that log ID and destination where the information for that log ID will be sent. You can think of a log ID as having inputs at one end from one or more of the four event streams and an output at the other end.

Optionally, you can create an event filter policy that defines whether to forward or drop an event based on match criteria.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the relationship between log event sources, the log ID filter, the log IDs and the log destination.

Events from one or more event sources that are not suppressed by the event controller or the optional filter policy are forwarded to one of the event log destination.

Event controller:

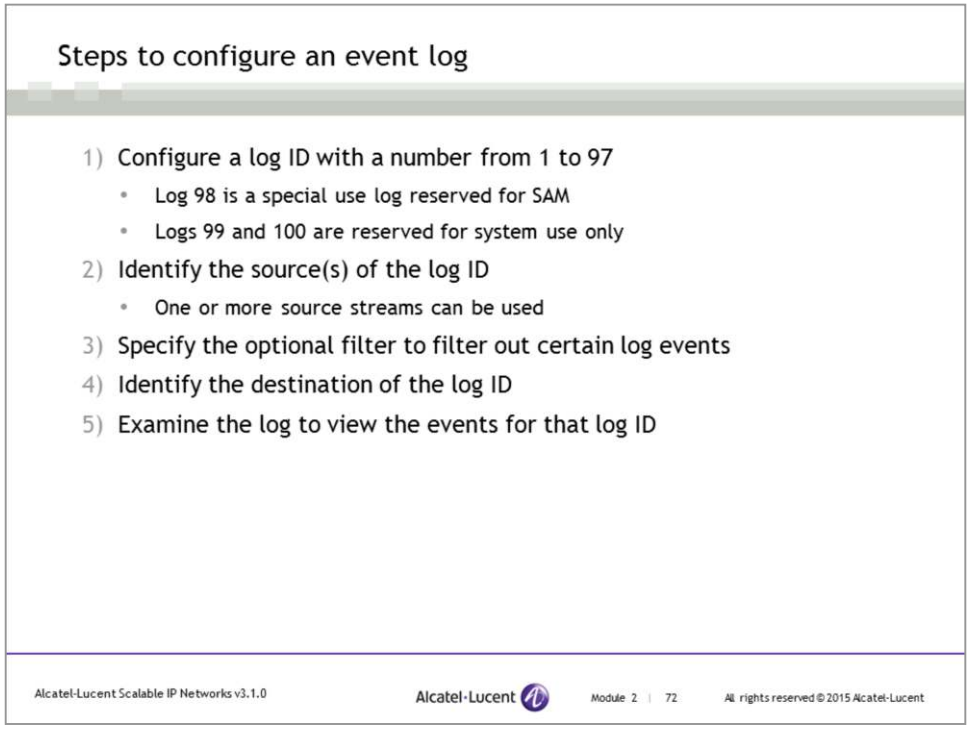
Event control pre-processes the events generated by applications before the events are passed into the main event stream. Event control assigns a severity to application events and can either forward the event to the main event source or suppress the event. Suppressed events are counted in event control, but these events will not generate log entries.

Event filter policy:

An optional event filter policy defines whether to forward or drop an event based on match criteria.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

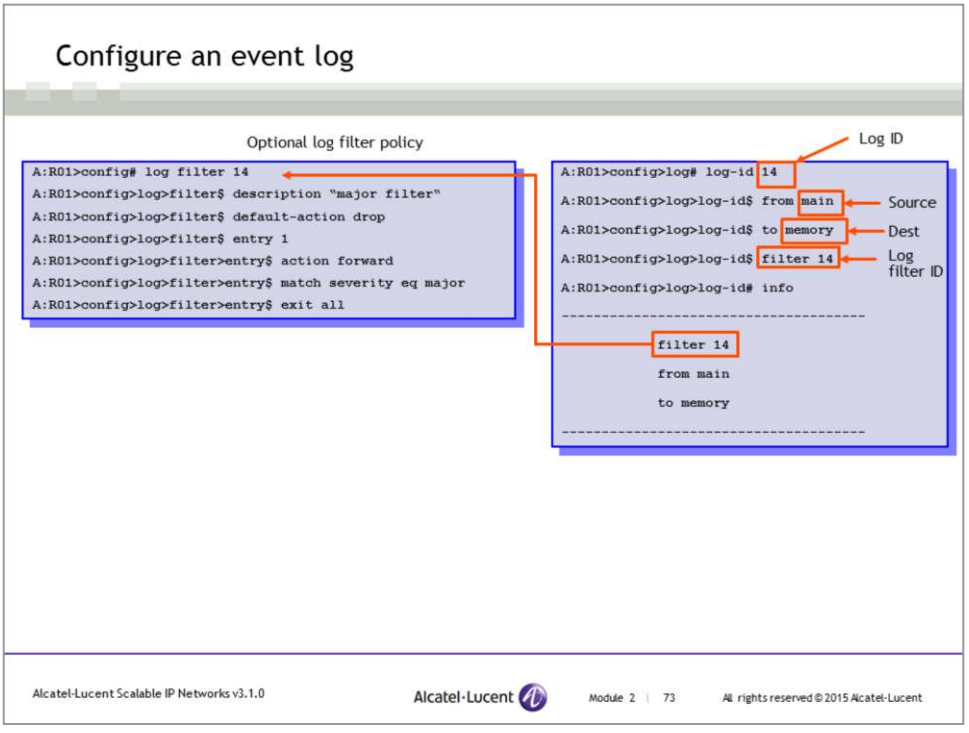
 All rights reserved © 2015 Alcatel-Lucent



This slide shows the five steps involved in configuring an event log.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

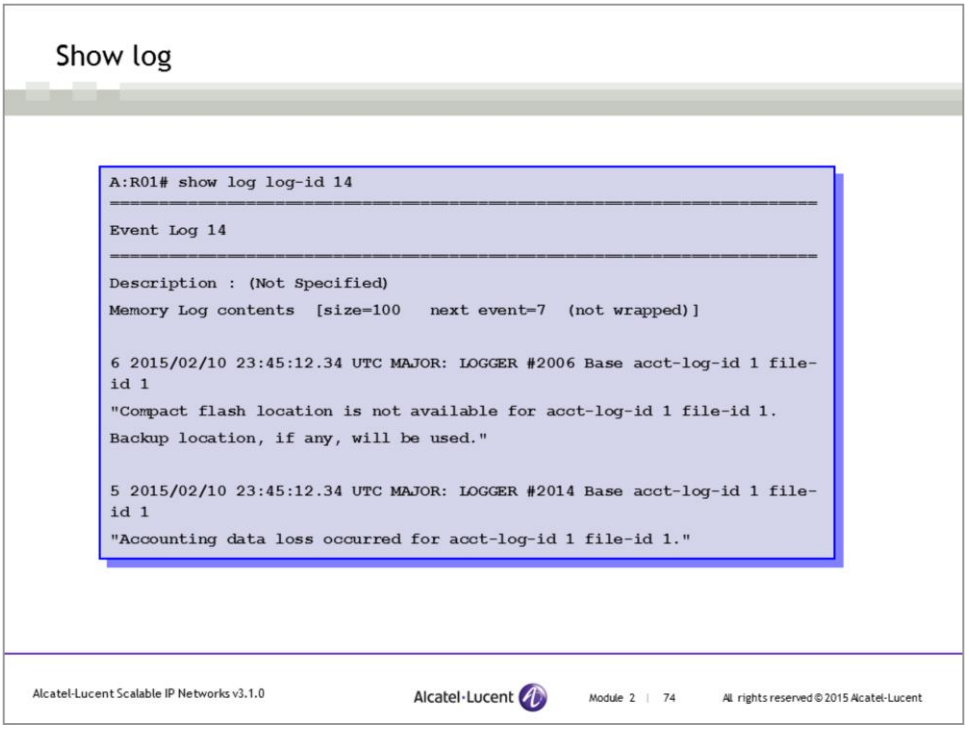


This slide shows an example of using the **log filter** command to create a filter for a log. A log is then created using the **log log-id** command and associated with the log filter defined.

A log filter 14 with a default action of drop is created. Only events with severity equal to major are forwarded.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The **show log log-id** command can be used to view information in a particular log ID. Since the logs can store a large amount of information, additional options are available to show only specific information in a log.

For example, the command **show log log-id 14 subject 1/1/1** displays information in the log about port 1/1/1 only.

You can use the **show log log-id ?** to see other options available to display the log information.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Module Summary

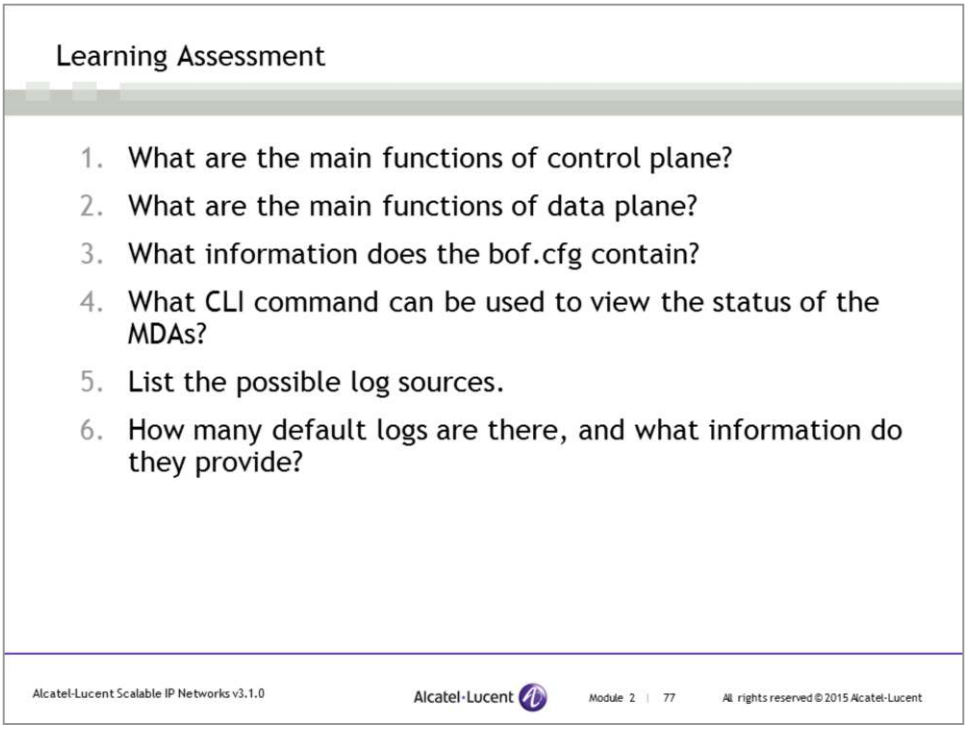
After successful completion of this module, you should be able to:

- Describe the functionality of the Alcatel-Lucent Service Router product family
- Describe the 7750 SR components
- Describe the bootup process
- Use the CLI commands
- Configure a basic router using the CLI
- Configure and display event logs

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent



Learning Assessment Answers

1. What are the main functions of control plane?

To support the management functions of the router, build the forwarding table information, and handle routing protocols messaging.

2. What are the main functions of data plane?

To receive, process and transmit user application traffic.

3. What information does the bof.cfg contain?

The bof.cfg file contains the locations of the image and configuration files (primary, secondary, and tertiary), as well as the management IP address, and the management port setting.

4. What CLI command can be used to view the status of the MDAs?

show mda

5. List the possible log sources.

main, security, debug, and change

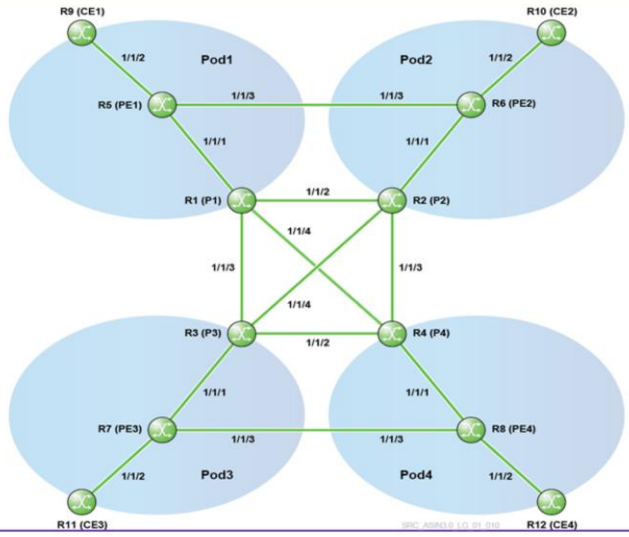
6. How many default logs are there, and what information do they provide?

Two default logs are pre-configured and reserved by the system. Log ID 99 contains all severity levels of events from the source main and log ID 100 only contains events with severity levels of major or critical from the source main.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Lab 1- Lab Infrastructure Configuration and Verification



 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Objectives

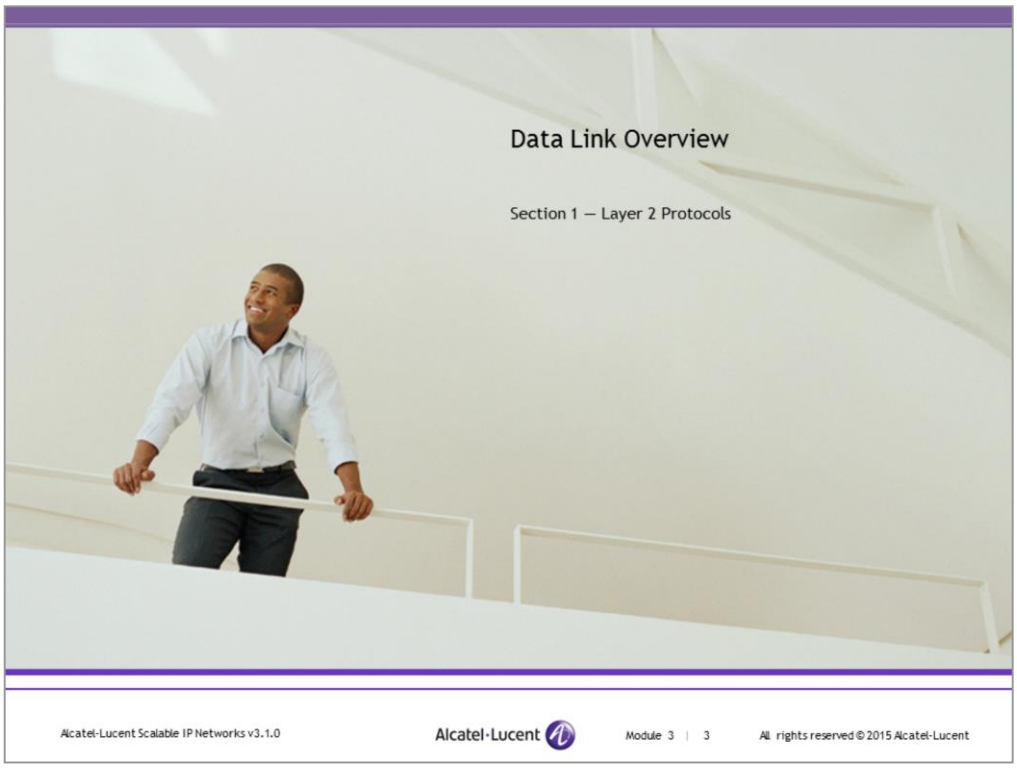
After successful completion of this module, you will be able to:

- Describe the characteristics of Layer 2
- Describe the characteristics of Ethernet
- List different types of Ethernet physical cabling
- Describe the purpose of a switch FDB and how it is populated
- Describe how a switch forwards unicast, multicast, and broadcast frames
- Describe different types of redundancy in an Ethernet-switched network
- Describe how virtual LANs can be used in one or more Ethernet switches

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

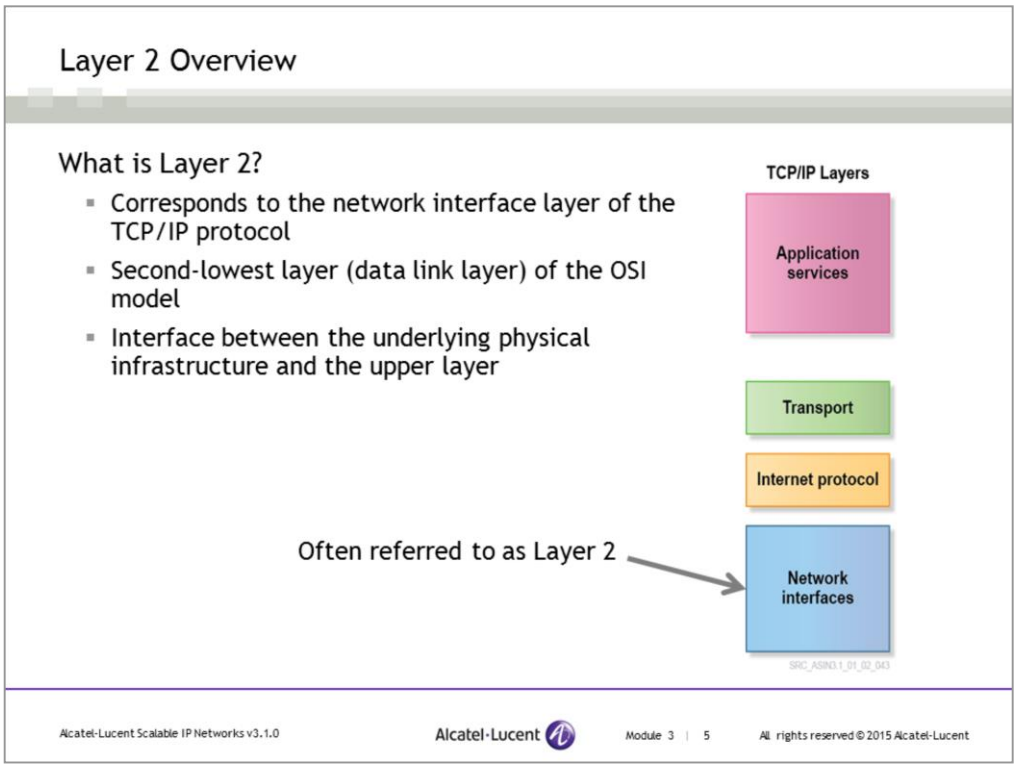
After successful completion of this section, you will be able to:

- Describe the scope of the data link layer
- Describe the operations of different Layer 2 protocols
- Describe how different Layer 2 protocols are used in a network

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



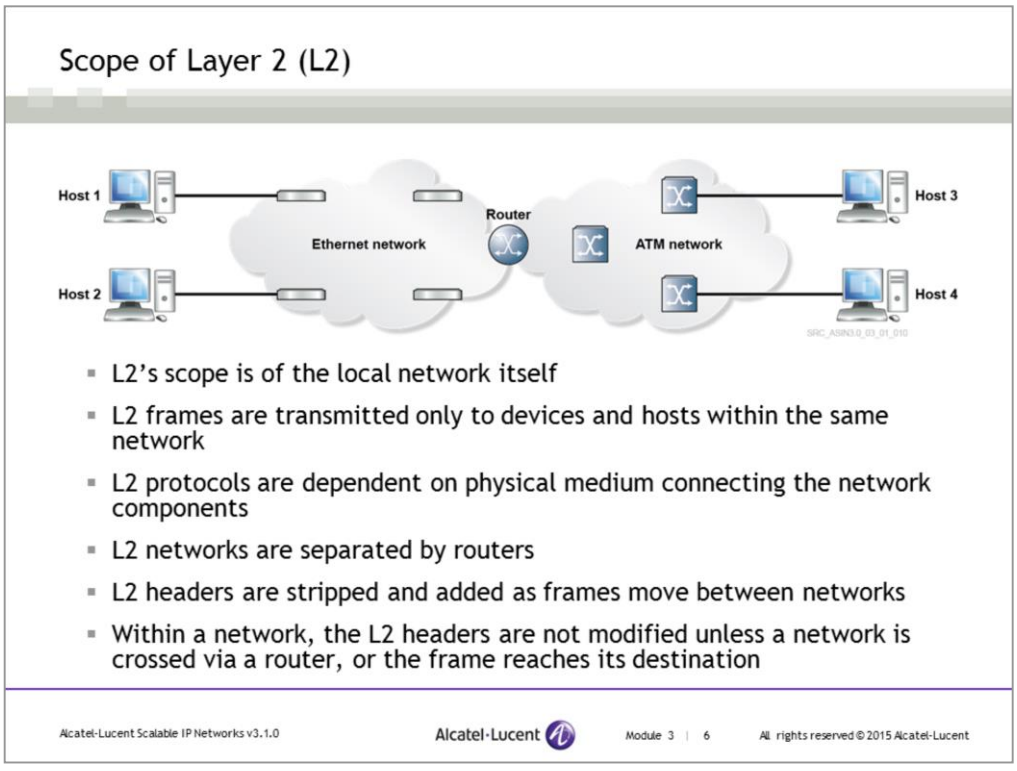
Layer 2 is the second lowest layer (data link layer) of the OSI (Open System Interconnection) model. Layer 2 corresponds to the network interface layer of the TCP/IP protocol. As discussed in module 1, each layer is responsible for a set of services and capabilities provided to the layers above and below it. Layer 2 is used to interact with the hardware and provides its own local addressing so that the upper layer does not need full understanding of the underlying physical infrastructure. With data encapsulation, Layer 2 hides the details of the interaction with the physical medium entirely from upper layer protocol such as IP.

The upper (IP) layer constructs a packet with an IP address that uniquely identifies the source and destination network device in the internetwork. The packet may then be transmitted over several different networks (same/different physical media) before it reaches its destination. In any one particular network, Layer 2 is responsible for encapsulating the packet into a frame for Layer 2 forwarding. The frame is stamped with a Layer 2 header, which contains Layer 2 source and destination addresses. When Ethernet is used, these Layer 2 addresses are called media access control (MAC) addresses. Layer 2 headers are stripped and added as frames move from one network to another network.

After adding the Layer 2 addresses to the frame, the Layer 2 passes the frame to the physical layer for transmission over the physical medium. The receiving network device must be able to recognize that the frame is destined for itself and verify that the packet is intact. Because the entire packet is transmitted over the physical medium, noise and other signal disturbances could corrupt or change the packet, rendering it meaningless to the higher-layer application.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The scope of a Layer 2 frame is the local network. For example, in a typical scenario of IP/Ethernet, each IP subnet is considered to be one network. The Layer 2 frame remains intact while it traverses the Layer 2 devices in a particular IP subnet. If the IP packet needs to be routed to another subnet via an IP router, the original Layer 2 frame is removed after it ingresses the IP router.

When forwarding the IP packet out from the appropriate port, the IP router constructs a new Layer 2 frame with correct headers and Layer 2 addresses. This new Layer 2 header is used as the frame traverses to the next subnet. This process continues until the destination host is reached.

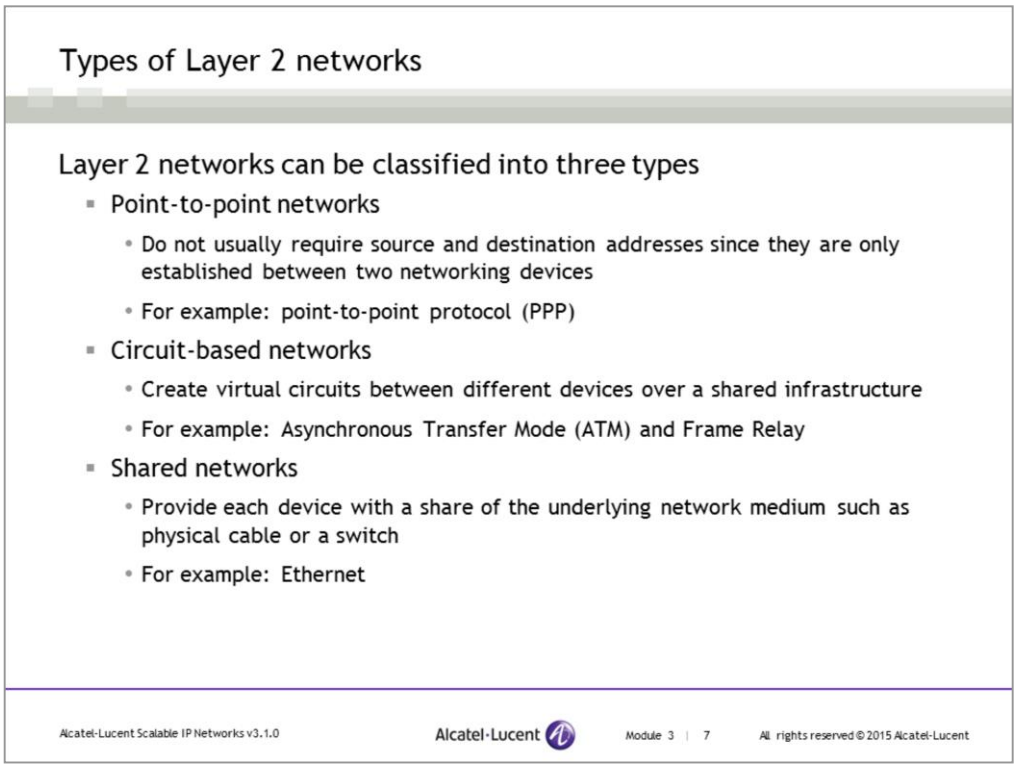
The application data sent between two host stations can traverse several physically different networks. Each network has a different Layer 2 header and may even use different Layer 2 protocols that depend upon the physical wire such as Ethernet, point-to-point protocol (PPP), ATM, or Frame Relay.

In this slide, hosts (PCs) on the Ethernet network communicate with each other using the Ethernet protocol, and hosts on the ATM network communicate with each other using the ATM protocol. A router is required for hosts using different L2 protocols to communicate with each other.

The end hosts on the Layer 2 network communicate with each other using the specific Layer 2 protocol. The PCs on the left side of the Ethernet network do not require anything other than Ethernet L2 framing to communicate with each other. Similarly, the PCs on the right side of the network require only ATM L2 framing to communicate with each other. The L2 networks are separated by routers, which are Layer 3 devices. The PCs on the Ethernet network can only communicate with the PCs on the ATM network using Layer 3 addresses. Note that the devices in the ATM cloud represent ATM switches; the devices in the Ethernet cloud represent Ethernet switches. The device connecting the two clouds is a router.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Layer 2 networks can be broadly classified into three types:

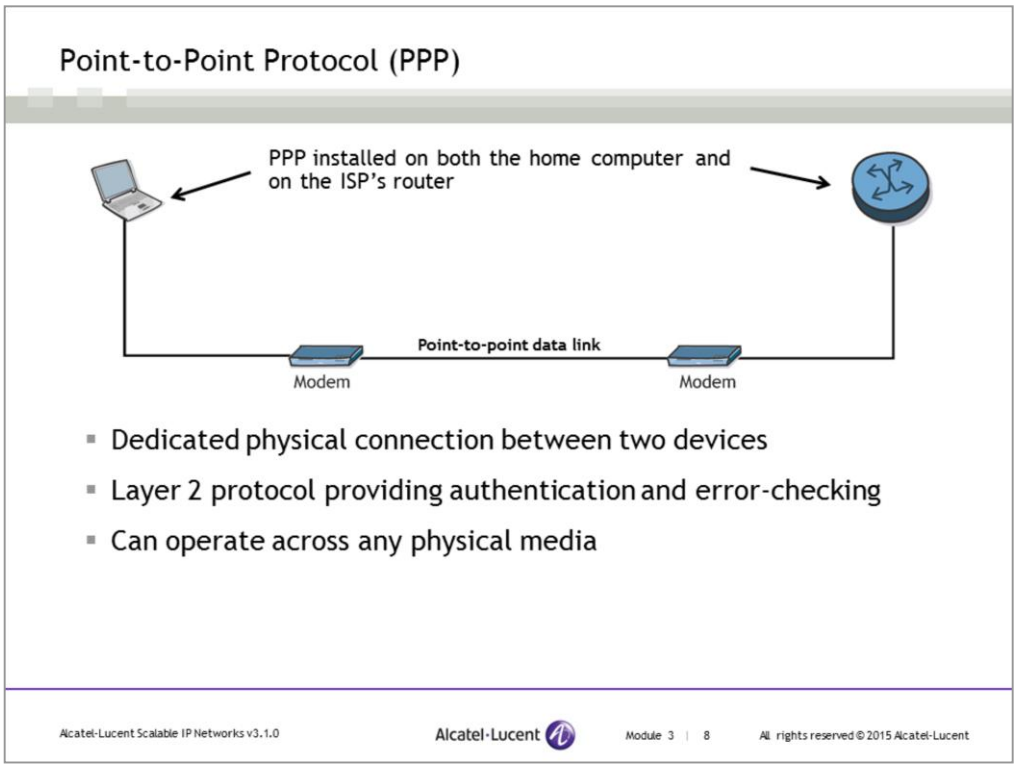
- Point-to-point networks - do not usually require source and destination addresses since they are established between two networking devices only
- Circuit-based networks – create virtual circuits between different devices over a shared infrastructure. Usually this involves manually mapping a path through network switches from one location to another.
- Shared networks – provide each device with a share of the underlying network medium such as physical cable or a switch. All devices can send and receive traffic to each other directly through the shared medium.

Layer 2 framing usually consists of:

- a circuit identifier in the case of circuit-based networks
- an address that directs the packet to the required destination, usually on shared media
- a fixed-length maximum size, maximum transmission unit (MTU) established between the source and receiving component; data from higher-layers is broken into fixed-length frames (covered later)
- an error check that is inserted by the source component and verified by the receiving component to maintain data integrity

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In previous periods in Internet development, point-to-point data links allowed hosts to communicate with each other through the telephone network. Older protocols such as SLIP (serial line IP) provided a simple mechanism for framing higher-layer applications for transmission along serial lines. SLIP, in accordance with RFC 1055, sent the datagram across the serial line as a series of bytes, and it used special characters to mark when a series of bytes should be grouped together as a datagram. SLIP was simple enough, but could not control the characteristics of the connection. Because of its limitation and lack of features such as error detection, SLIP has largely been replaced by other protocols such as point-to-point protocol (PPP).

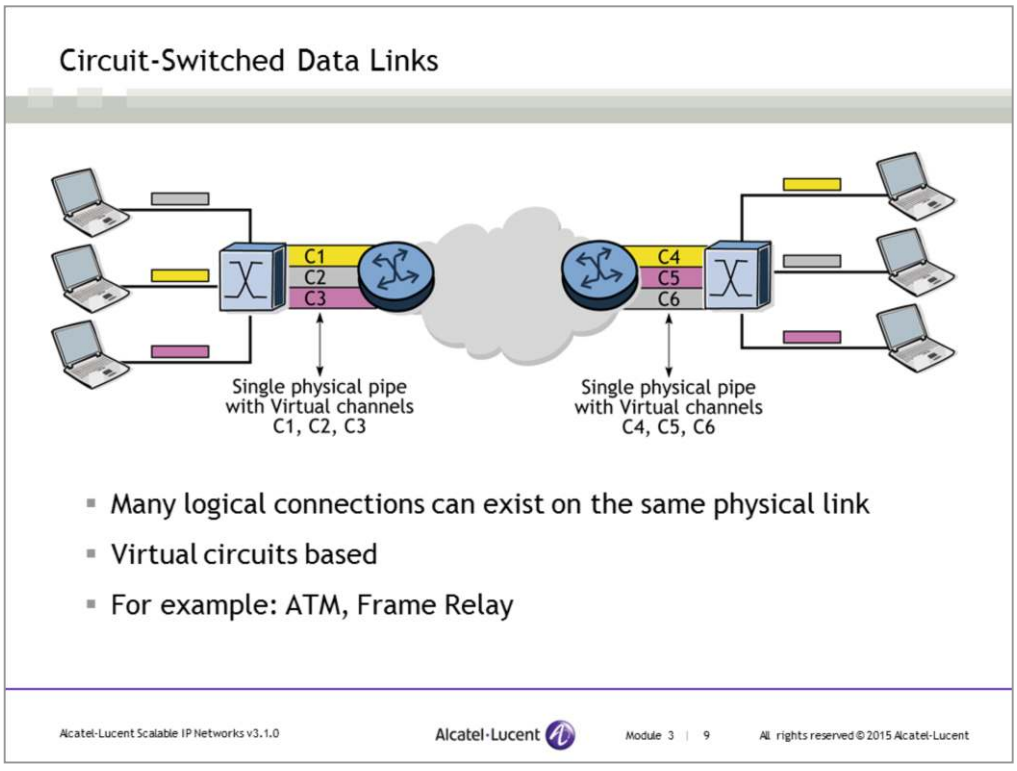
Today, the protocol of choice is PPP, which provides advantages such as link control to negotiate link characteristics, network control to transfer multiple Layer 3 protocols, and authentication used by remote computers to dial into their Internet service.

This slide shows a typical configuration for PPP installed on your home computer and on the ISP's router.

Please refer to RFC 1661 on details about point-to-point protocol.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

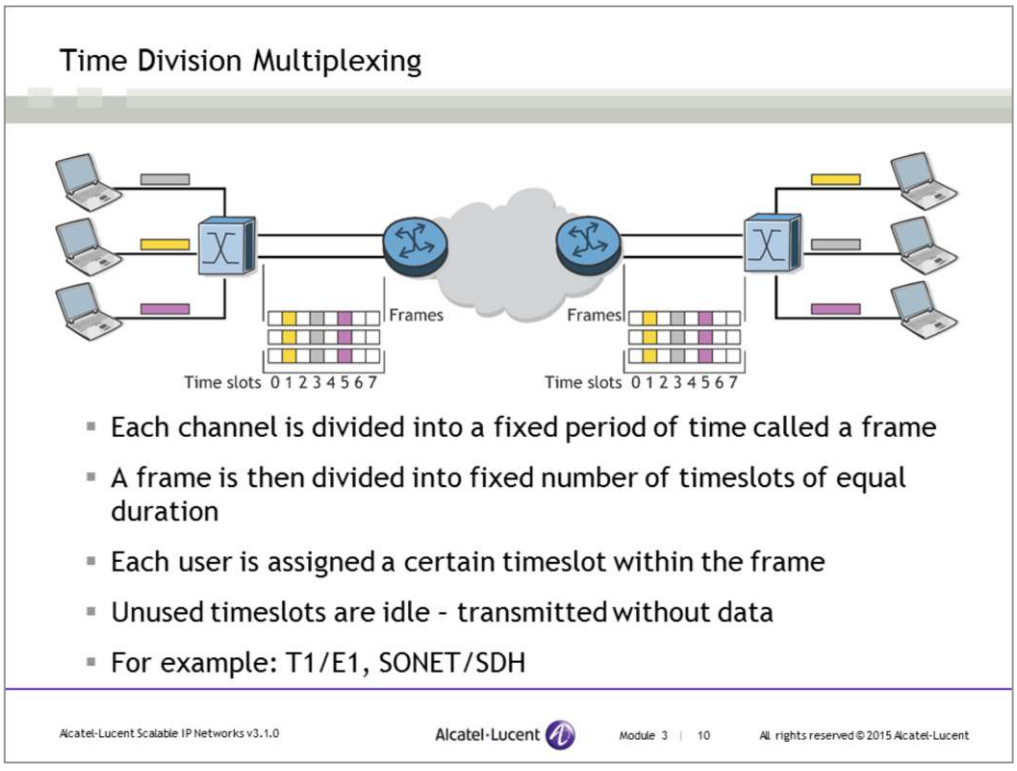


Circuit-switched protocols allow the transfer of user information as a unique set of packets identified by virtual circuits.

In the slide, the switch on the left accepts traffic from each host PC into a virtual circuit and switches to another virtual circuit when going to the router. The virtual circuit number is the same between the host PC and the switch, and between the switch and the router. Traffic from each PC is uniquely identified by a virtual circuit at every hop. This allows for many logical connections to be configured over a single physical connection and is the predominant way that WAN connections are handled in modern networks.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Time Division Multiplexing (TDM) is a digital technology where individual signals are interleaved into a composite multiplexed signal. Recurring fixed-length time slots are created such that each individual signal is represented by one channel or by multiple channels. The time slots allocated for each user occurs at the same time for every frame. Users can access the channel only when a time slot that has been allocated to them is available. If there is no traffic ready to send when the designated timeslot occurs, that timeslot is unused. If a user has a burst of traffic that exceeds the capacity of the designated time slots, additional slots cannot be used, even if they are idle. As a result, a long delay could result before the burst of traffic is transferred over the TDM network.

The total transmission bandwidth is split among the time slots. The total composite signal includes the payload bits for the composing channels and overhead bits.

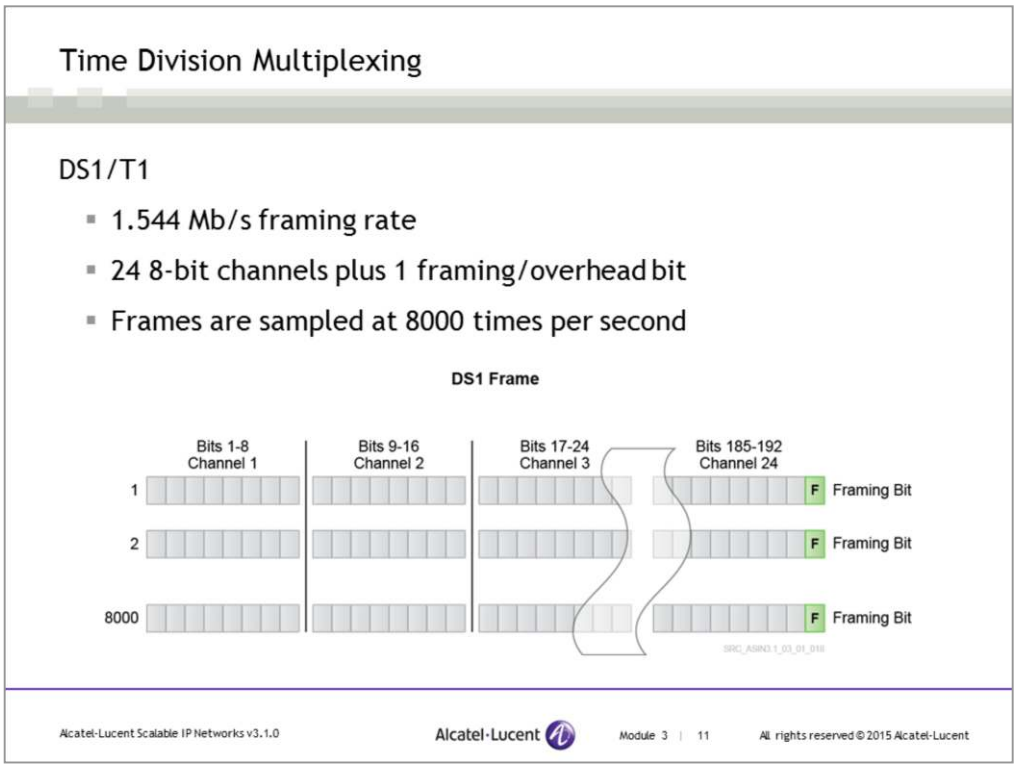
Each host PC sends information to the switch. The switch then transmits a frame to the router at a constant data rate (for example, 1.5 Mbps). On a T1, the frame is divided into many fixed time slots (24); each slot contains 64 Kb. Each host can occupy one or more time slots per frame.

The key point is that each host PC is given a fixed data rate. If the host uses one timeslot, then its transmitting rate is 64 Kbps. If the pipe rate is 1.5 Mbps, the host will have to supply their 64 Kbps in the next frame. The TDM designation is used because each host gets a fixed amount of time, and those times are multiplexed onto the same physical channel.

In this slide, each host PC transmits its characteristic frame (grey, yellow, purple). The frames that are transmitted from the switch containing several fixed-length timeslots. Within each of these frames, three of the timeslots are used by the respective host PCs. At the receiving switch, these frames are reassembled into three different frames and sent to the receiving PC.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

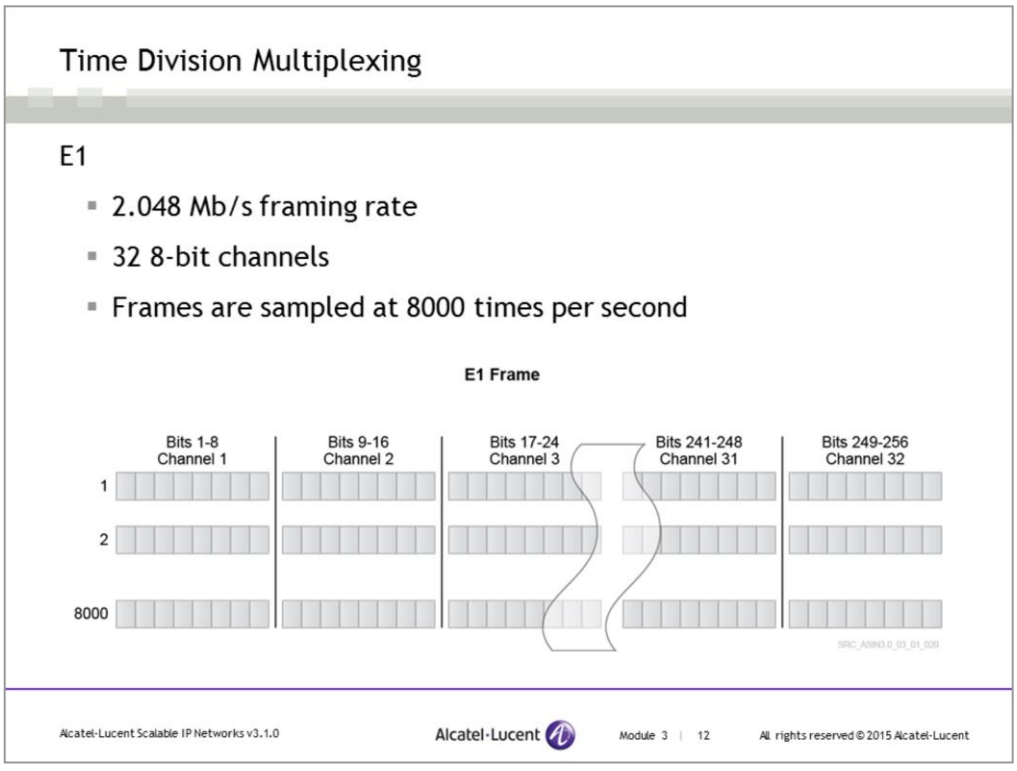


The frame structures of the DS1 [ANSI95b] are shown above. The DS1 signal consists of 24 payload channels plus overhead. The basic frame of each of these signals repeats every 125 µs, that is, 8000 times per second. With 8 bits carried in each channel, this gives rise to a basic data rate of 64 kbps for each channel. The requirement for this data rate stems from the need to sample the analog telephony signal 8000 times per second and encode each sample in 8 bits. A DS1 frame contains 24 channels, each consisting of 8 bits, plus 1 framing/overhead bit, leading to a total of 193 bits. Because the frame repeats every 125 µs (or 8000 times a second), the total bit rate of the DS1 signal is 1.544 Mbps.

The framing/overhead bit is used to transmit framing and clocking information.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



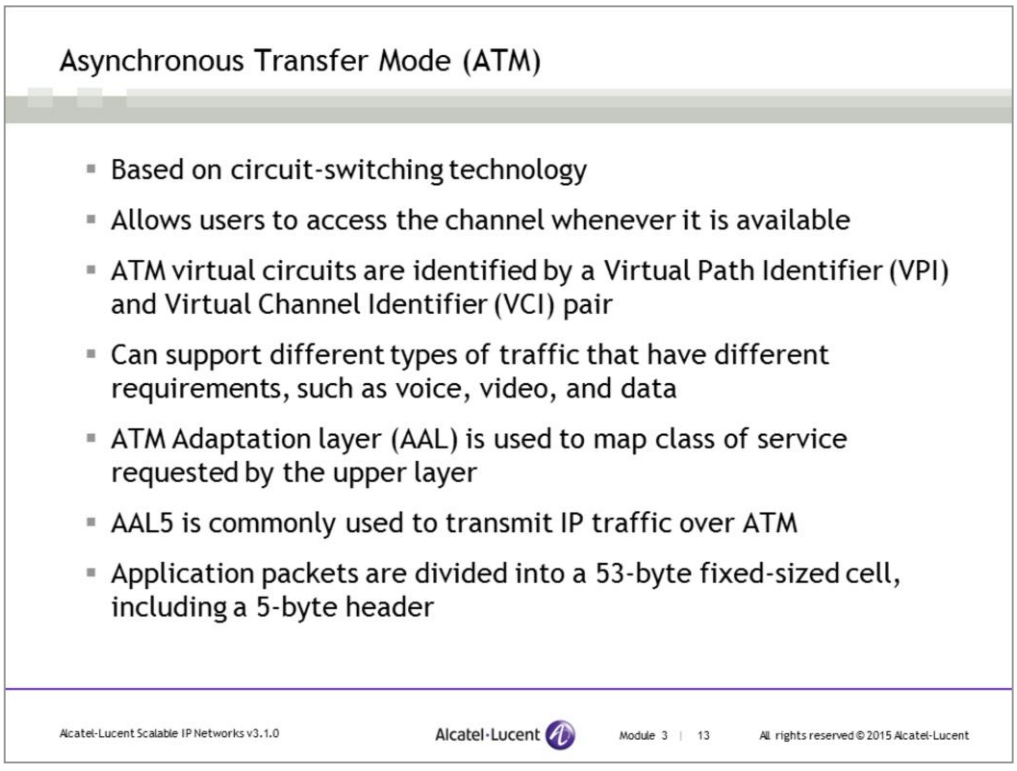
The frame structures of the European E1 [ITU-T98a] signals are shown above. The E1 signal consists of 32 payload channels. The basic frame of each of these signals repeats every 125 µs, that is, 8000 times per second. With 8 bits carried in each channel, this gives rise to a basic data rate of 64 kbps for each channel. The requirement for this data rate stems from the need to sample the analog telephony signal 8000 times per second and encoding each sample in 8 bits. An E1 frame contains 32 channels, each consisting of 8 bits, leading to a total of 256 bits. Because the frame repeats every 125 µs (or 8000 times a second), the total bit rate of the E1 signal is 2.048 Mbps.

It is important to know two channels are reserved. Channel 0 is reserved for transmission management. Channel 16 is reserved for signalling. The differences between T1 and E1 is the number of channels but the speed remains the same.

E1 is a European standard and T1 is North American standard.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In contrast to TDM, ATM allows user to access the channel whenever it is available. ATM does not impose a pattern or rule on the way users are given access to the channel.

ATM packets are further encapsulated by ATM adaptation layers (AAL), which are responsible for the segmentation and reassembly (SAR) of ATM cells of higher-layer data received at the other end. The purpose of this is to adapt the class of service from higher-layers onto connectionless ATM cells. The AAL classification is related to the service and application required for transport. Usually the following adaptation layers are mapped to the following classes of service:

- AAL1 – Constant Bit rate service
- AAL2 – Variable Bit rate service
- AAL3/4 – Connection-oriented data usually
- AAL5 – Connectionless data service usually (for example, IP)

Constant Bit Rate (CBR) service: AAL1 encapsulation supports a connection-oriented service where minimal data loss is required. Examples of this service include 64 Kbps voice, fixed-rate uncompressed video, and leased lines for private data networks.

Variable Bit Rate (VBR) service: AAL2 encapsulation supports a connection-oriented service in which the bit rate is variable but requires a bounded delay for delivery. Examples of this service include compressed packetized voice or video. The requirement on bounded delay for delivery is necessary for the receiver to reconstruct the original uncompressed voice or video.

Connection-oriented data service: For connection-oriented file transfer and data network applications where a connection is set up before data is transferred, this type of service has variable bit rate and does not require bounded delay for delivery. Two AAL protocols were defined to support this service class and have been merged into one type: AAL3/4.

Connectionless data service: Examples of this service include datagram traffic and data network applications where no connection is set up before data is transferred. Connectionless data service is used to transport IP/Ethernet/Frame Relay applications.

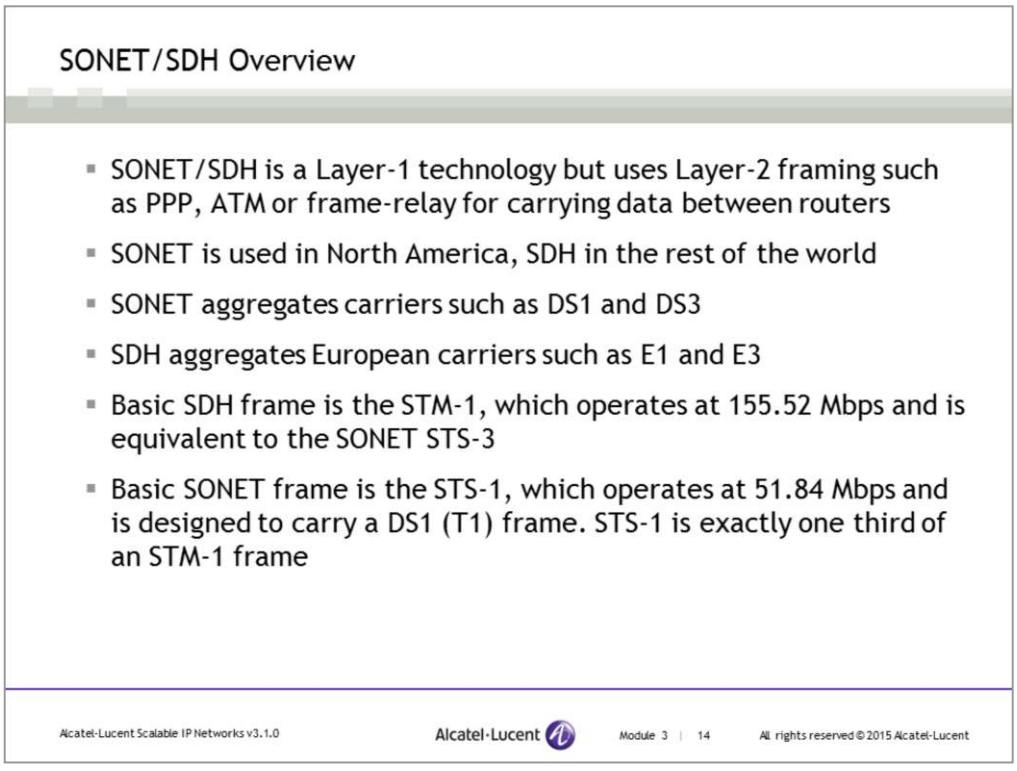
Higher-level Service Delivery Units (SDUs) may be several bytes in length. However, as the ATM payload is only

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

48 bytes, the SDU must be segmented into multiple cells as it enters the ATM network, then reassembled when it exits the ATM network. This function of the ATM adaptation layer is known as SAR. The adaptation layer comprises two sublayers, one of which is the SAR sublayer, the other being the convergence sublayer (CS), which performs service-dependent functions.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Synchronous optical network/Synchronous Digital Hierarchy (SONET/SDH) is a high-bandwidth WAN transport technology developed by Bell Communications Research and later standardized by ANSI and ITU. SONET/SDH is synchronous in nature and specifies framing and multiplexing at the physical layer of the OSI model. SONET/SDH was originally designed to transport voice but has been adapted to transport data by using Layer 2 framing technologies such as PPP/HDLC and ATM.

SONET/SDH technology is typically not implemented by small or medium-sized businesses, because of its high cost. It is more commonly used by large global companies, long-distance companies linking metropolitan areas and countries, or ISPs that need to guarantee fast, reliable access to the Internet. SONET/SDH is particularly suited to audio, video, and imaging data transmission. As you can imagine, because of its reliance on fiber-optic cable and its redundancy requirements, SONET/SDH technology is expensive to implement.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

SONET/SDH Overview (continued)

- Basic SONET frame is known as STS-1 at 51.84 Mbps
- Each STS-1 can carry one DS3 frame
- STM-1 frame is the equivalent of the STS-3 frame and is designed for European carriers
- Higher levels achieved by combining exact multiples of STS-1 and STM-1

	Bit rate (Mbps)	SONET frame	DS3s	DS1s	DS0s	SDH frame	E3s	E1s	E0s
OC-1	51.84	STS-1	1	28	672	STM-0	1	16	512
OC-3	155.52	STS-3	3	84	2016	STM-1	4	64	2048
OC-12	622	STS-12	12	336	8064	STM-4	16	256	8192
OC-48	2488	STS-48	48	1344	32 256	STM-16	64	1024	32768
OC-192	9953	STS-192	192	5376	129 024	STM-64	256	4096	131072

All rights reserved © 2015 Alcatel-Lucent

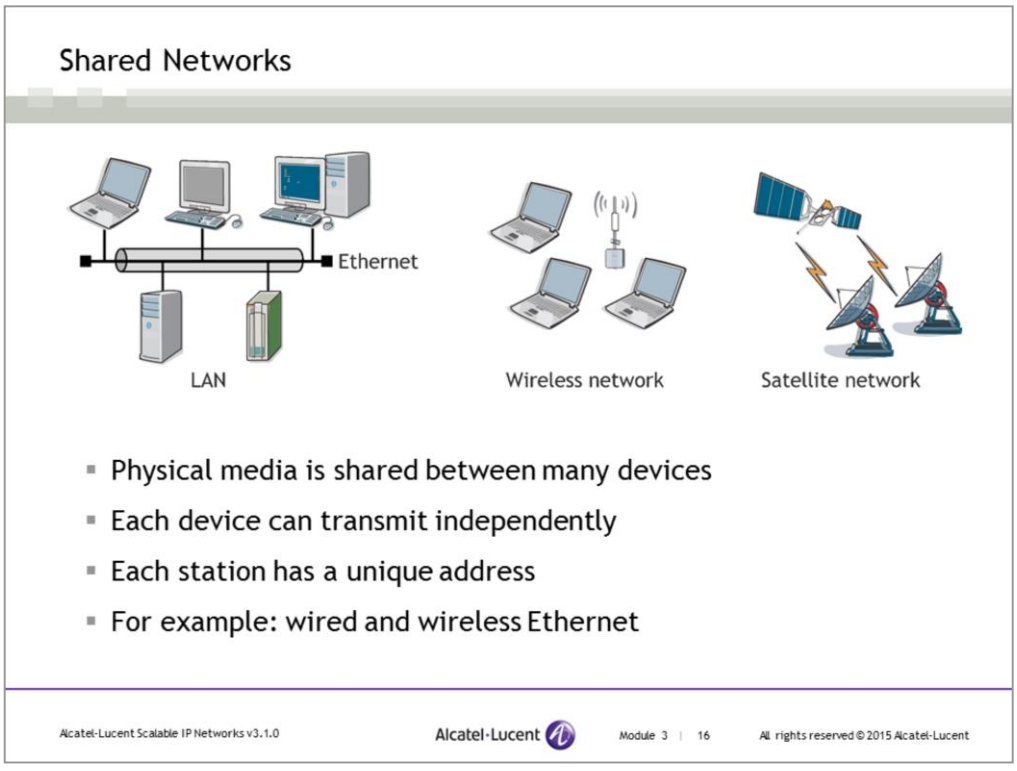
The basic SONET signal is known as synchronous transport signal (STS-1) and has a bit rate of 51.84 Mbps. This includes a payload of 50.112 Mbps and an overhead of 1.728 Mbps. The STS-1 frame is 810 bytes and is transmitted in 125 ms, hence the bit rate of 51.84 Mbps.

Each STS-1 can carry one DS3 or twenty-eight DS1 frames. For higher data rates, the STS-1 signal is incremented at fixed levels to STS-3, STS-48, and STS-192. Multiplexing can occur in one or multiple stages. For example, an STS-12 can be formed by four STS-3s, twelve STS-1s, three STS-3s or three STS-1s. Each STS-1 payload in a SONET frame is assigned a fixed position and can be extracted without having to fully de-multiplex the entire frame. This is a very big advantage of SONET compared to DS3.

The STM frames (STM-1, and so on) used by SDH are effectively a multiple of STS-3 frames. The overhead is identical, although the terminology and overhead usage varies somewhat between the standards. STM-1 is designed to carry an E3 frame. A number of different standards have been defined for the multiplexing of lower data rates within STS-1 or STM-1 frames.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

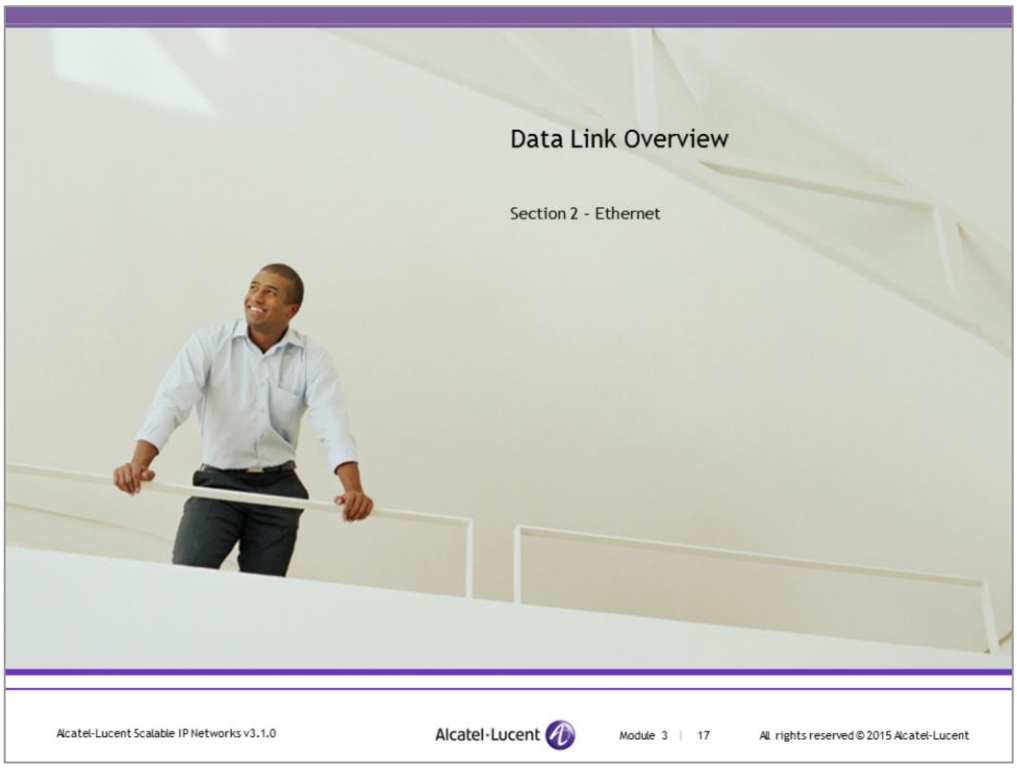


Broadcast networks typically use shared media to communicate to all the devices that are attached to that shared media. For data to be reliably delivered from the source to the destination, each of the devices on the shared media is identified by a particular address. The frame that is sourced from the sending device is sent to all the devices sharing the media (broadcasting). All devices will receive the frame but only the device whose address appears in the frame as the destination address will interpret the data. The rest of the devices will ignore the data.

To transmit data reliably, the sending device on the shared media must compose the frame, obtain control of the media, and transmit the information. Because the media is shared, it is possible for multiple stations to transmit their information simultaneously, resulting in a collision. This collision causes data corruption. Depending on the protocol used, an algorithm needs to be followed to ensure a minimum number of collisions and also to ensure proper recovery from collisions. An example of a shared media protocol that is very commonly used today is Ethernet.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

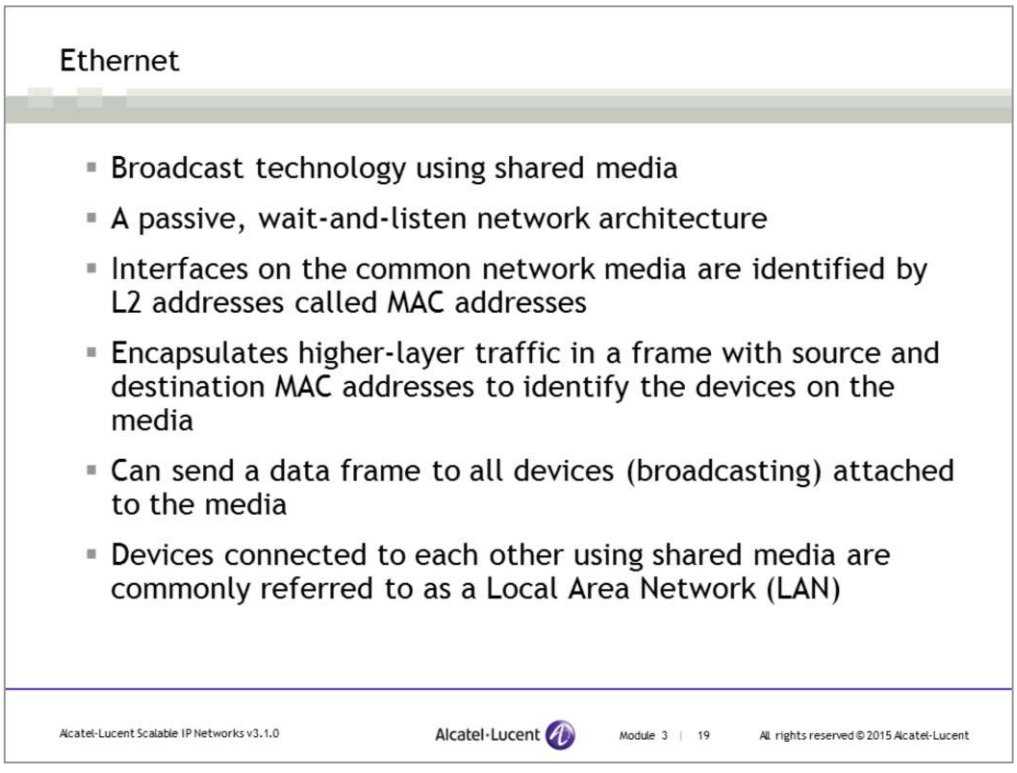
After successful completion of this section, you will be able to:

- List the characteristics of Ethernet
- Compare the two Ethernet frame standards: Ethernet II and 802.3
- Describe the functions of key fields in an Ethernet frame

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

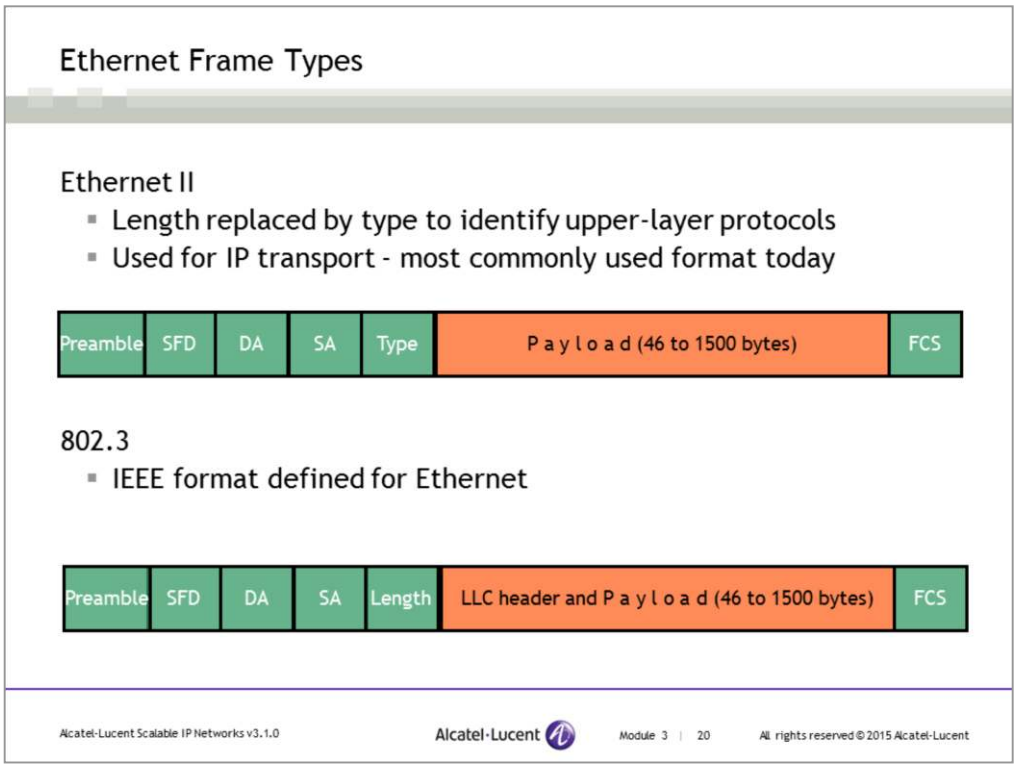
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Computers must contend for transmission time on the network media. In fact, Ethernet is commonly described as a contention-based architecture.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Ethernet supports two frame types, but they have been standardized so that all types can be transmitted on a common Ethernet network. The 16-bit field that follows the source address (SA) indicates whether the frame is Ethernet II or 802.3. If the value is 1536 or less, the frame is treated as 802.3. If the value is greater than 1536, the frame is treated as Ethernet II.

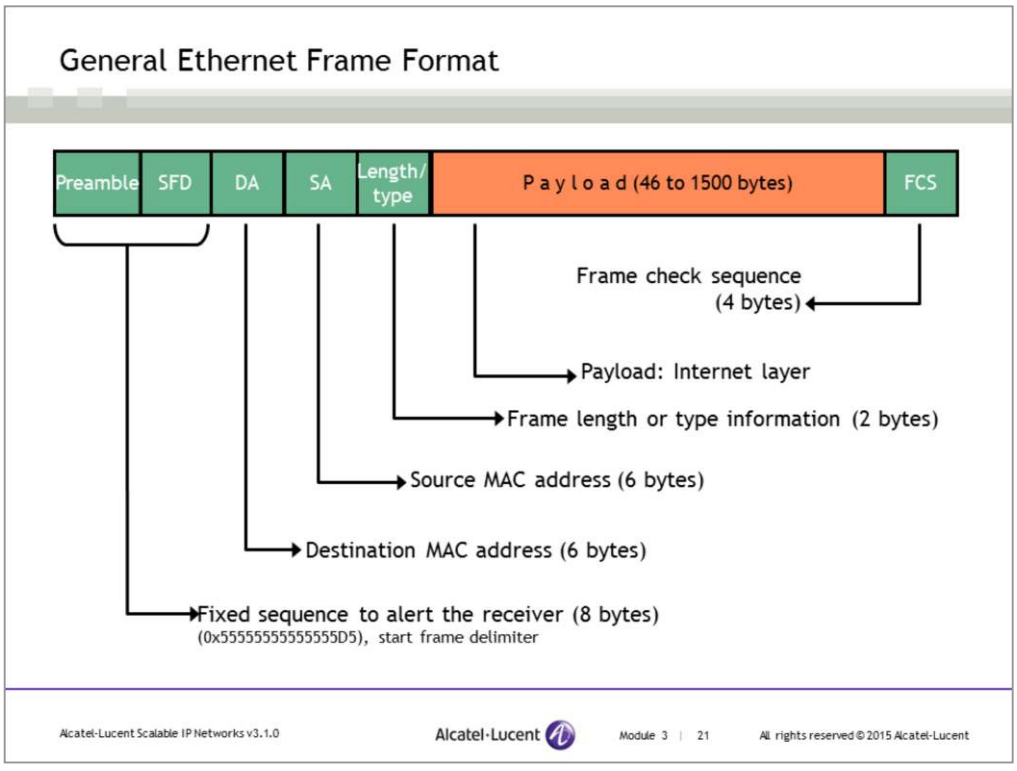
Ethernet II was originally developed by Digital, Intel, and Xerox in 1980 and is commonly known as the DIX standard. It was adopted by the IEEE and went through formal standardization to form the 802.3/802.2 frame types. The Ethernet II frame is usually used for transmission of IP datagrams.

Ethernet 802.3 was developed by the IEEE from the original Ethernet standard in 1983. IEEE Ethernet defines two layers; the lower MAC layer in 802.3 and an upper LLC (logical link control) layer in 802.2. These are sublayers of the OSI data link layer (Layer 2). The two layers were defined separately to provide additional link control features, and so that common LLC frames could be used for different media types, such as Ethernet, Token Ring and FDDI. This allows bridging at Layer 2 between different media types.

There are three different 802.3 formats that were used for older protocols, such as Novel Netware's IPX, Apple Computer's Appletalk protocols and OSI protocols. Today, these formats are rarely used. The Alcatel-Lucent 7750 SR uses 802.3 for the transmission of IS-IS routing updates; however, it uses Ethernet II for other traffic, such as IP and MPLS.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The frame consists of a set of bits organized into several fields. These fields include address fields, a variable-size data field that carries from 46 to 1500 bytes of data, and an error checking field that checks the integrity of the bits in the frame to make sure that the frame has arrived intact. The original Ethernet standards defined the minimum frame size as 64 bytes and the maximum as 1518 bytes. These numbers include all bytes from the destination MAC address field to the frame check sequence field. The preamble and the start frame delimiter fields are not included when quoting the size of a frame. The IEEE 802.3ac standard released in 1998 extended the maximum allowable frame size to 1522 bytes to allow for a VLAN tag to be inserted into the Ethernet frame format. Gigabit Ethernet and 10 gigabit Ethernet ports may support jumbo frames, which can be 9000 bytes.

Preamble: A stream of bits that allows the transmitter and receiver to synchronize their communication. The preamble is a 56-bit long pattern of alternating ones and zeroes. The preamble is immediately followed by the Start Frame Delimiter.

Start Frame Delimiter (SFD): Always 10101011 and used to indicate the beginning of the frame information.

Destination MAC (DA): The MAC address of the machine receiving data.

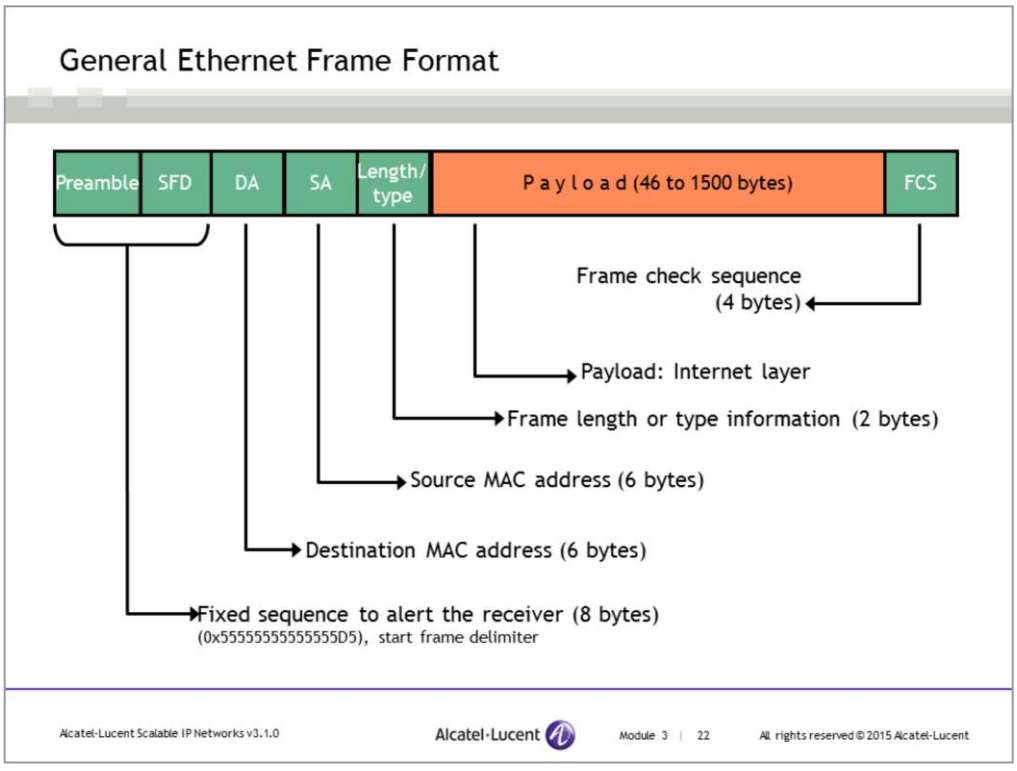
Source MAC (SA): The MAC address of the machine transmitting data.

Length/Type: The payload length or type field, also known as Ethertype. If the Ethernet frame is in the 802.3 format, this field is interpreted as length. If the Ethernet frame is in the Ethernet II or original DIX format, the field is interpreted as type, or Ethertype. The numeric value in this field determines whether the frame is an 802.3 frame or Ethernet II frame. If the value is less than 1536, it is an 802.3 frame. If the value is 1536 or greater. it is an Ethernet II frame.

(. . . continued on next slide)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



(. . . continued from previous slide)

Data/Padding (also known as Payload): This is where the IP header and data are placed if you are running IP over Ethernet. This field contains IPX information if you are running IPX/SPX (Novell). There are four specific fields in the payload section of an IEEE 802.2 frame:

- DSAP - Destination Service Access Point
- SSAP - Source Service Access Point
- CTRL - Control bits for Ethernet communication
- NLI - Network Layer Interface

An Ethernet frame must be a minimum of 64 bytes. Therefore, if the data field is less than 46 bytes in length, padding is included to bring the frame length to 64 bytes.

Frame Check Sequence (FCS): A part of the frame that verifies that the information each frame contains is not damaged during transmission. If a frame is damaged during transmission, the FCS on the frame will not match with the recipient's calculated FCS. The FCS is calculated by the sender based on the entire contents of the frame. The recipient calculates an expected FCS value on the frame that it receives. Any frames that do not match the calculated FCS are discarded.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

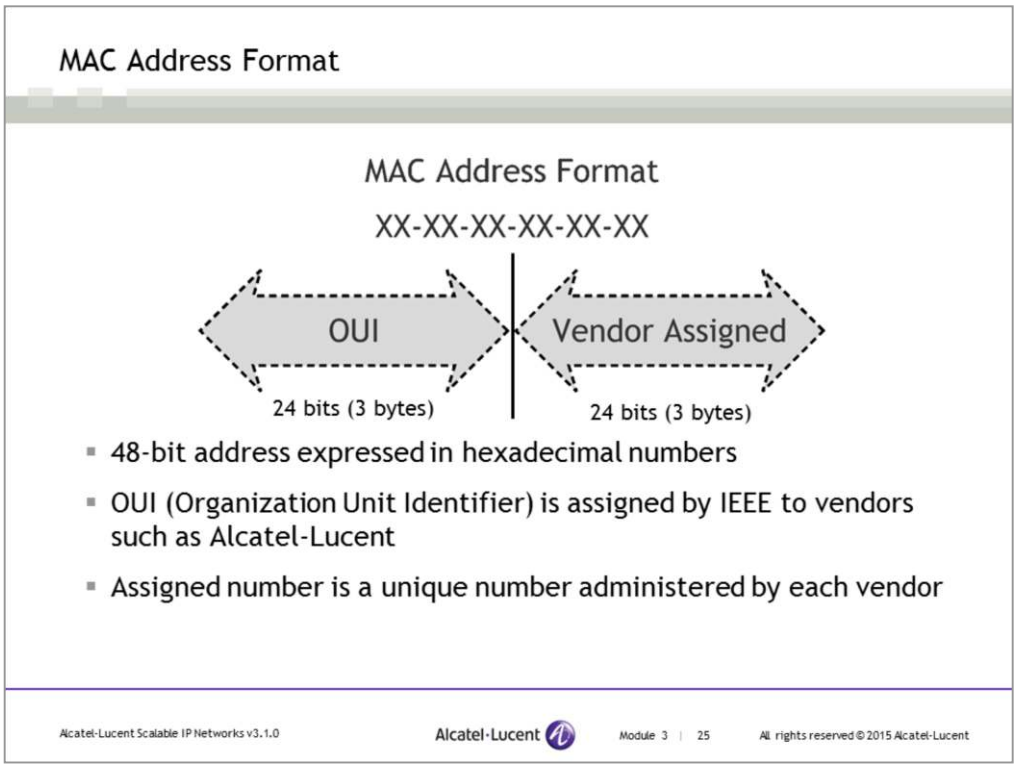
After successful completion of this section, you will be able to:

- Describe the Ethernet MAC address components
- Describe the format of MAC unicast, broadcast, and multicast addressing
- Describe the two different Ethernet transmission modes
- List available speed and operation modes for auto-negotiation

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 3 | 24
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

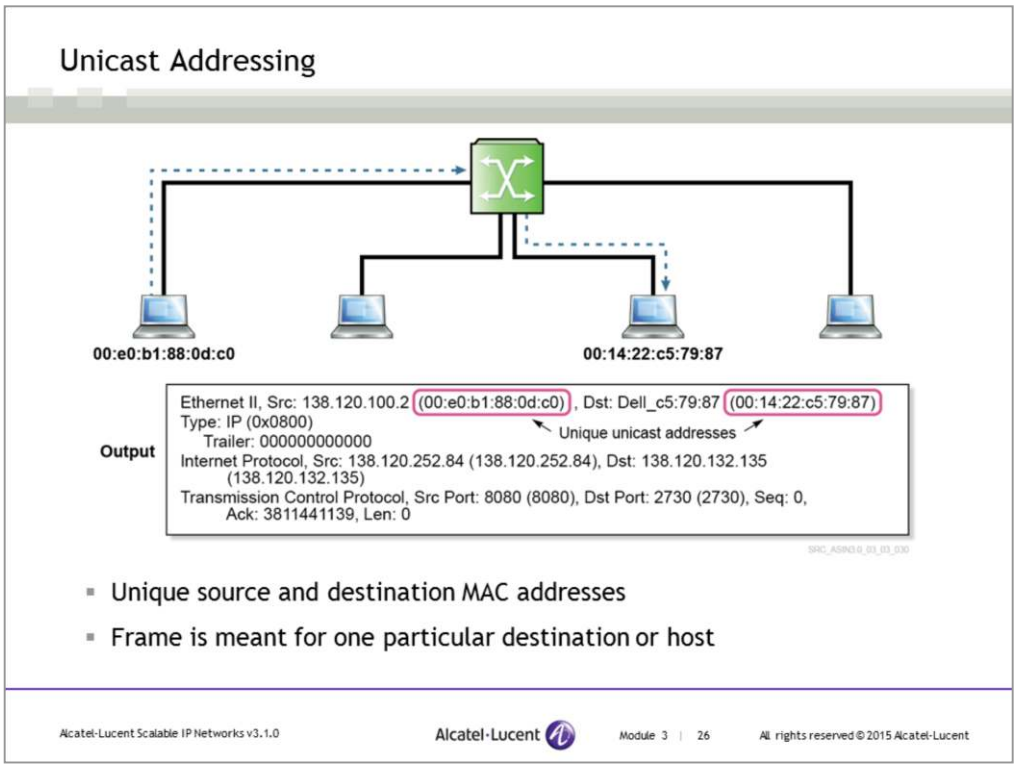


An Ethernet MAC address is a 48-bit (6 bytes) hexadecimal number consisting of two parts: the Organization Unit Identifier (OUI) , used to identify the card's manufacturer, and a vendor assigned number. Each portion of the MAC address is 3 bytes. A MAC address is usually displayed in dashed hexadecimal notation.

The OUI number is assigned by IEEE to vendors such as Alcatel-Lucent. For example, Alcatel-Lucent Canada has an OUI of 00-80-21, Alcatel-Lucent USA has an OUI of 00-17-CC, and Alcatel-Lucent Italia has an OUI of 00-20-60. A list of various vendors' OUIs can be found at the IEEE website http://standards.ieee.org/regauth/oui/index.shtml.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



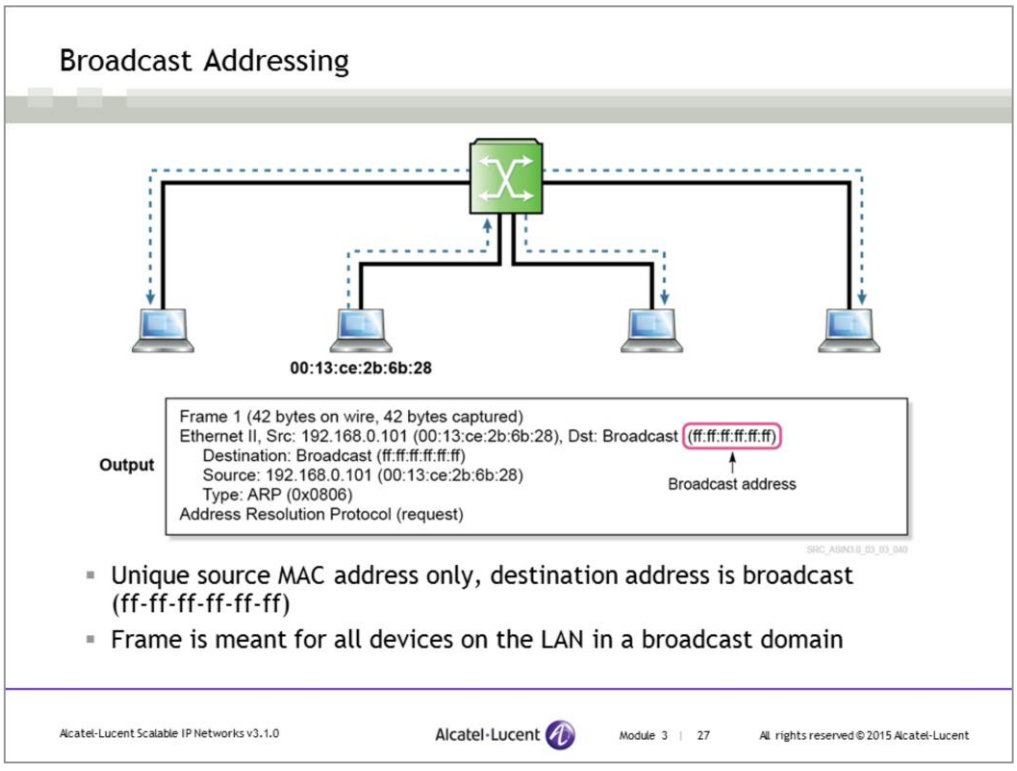
In this slide, the Ethernet source and destination addresses are shown as below

- Src : 00:e0:b1:88:0d:c0
- Dest : Dell_c5:79:87 (00:14:22:c5:79:87)

The frame is sent to a switch that connects all four devices. Assume the switch knows where to send the frame given a destination address. The switch will send the frame out of the appropriate port. Only the device whose MAC address matches the destination address accepts the frame. This mode of addressing is called unicast because only a single device is the intended destination.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



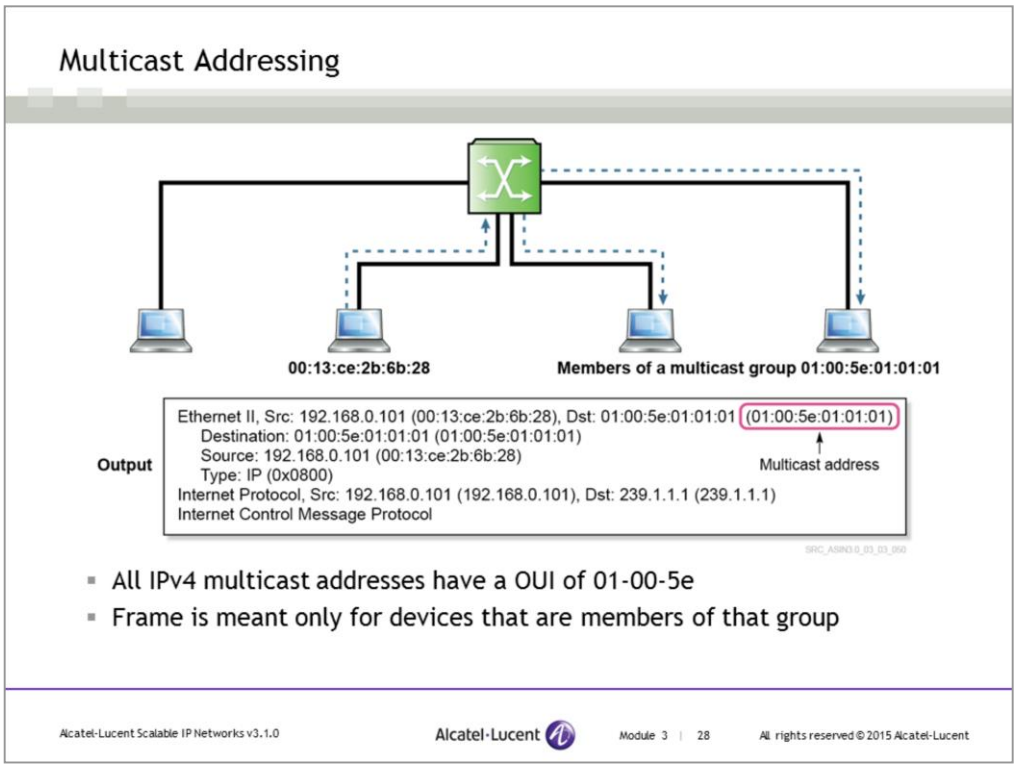
In this slide, the Ethernet source and destination addresses are shown as below

- Src : 00:13:ce:2b:6b:28
- Dest : ff:ff:ff:ff:ff:ff

The frame is sent to a switch that connects all four devices. When the switch receives the frame with a broadcast address, it sends the frame out on all its ports except the port where the frame was received (the port attached to the source). All devices recognize that the destination address (ff-ff-ff-ff-ff-ff) is a special address that means “all nodes” and process the frame.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, the Ethernet source and destination addresses are shown as below

- Src : 00:13:ce:2b:6b:28 (unique MAC address)
- Dest : 01-00-5e-01-01-01 (multicast group address)

The destination MAC address is modified to use the reserved multicast range. The range has the first 24 bits of the MAC address, normally reserved for the manufacturer code, set to an OUI of 01-00-5E. In the remaining 24 bits of the MAC address (01-00-5E-XX-XX-XX), the first bit is set to 0 (to indicate a multicast address) and the remaining 23 bits are the lower 23 bits of the IP multicast address. So in this example the conversion between the IP multicast address and the MAC address is as follows:

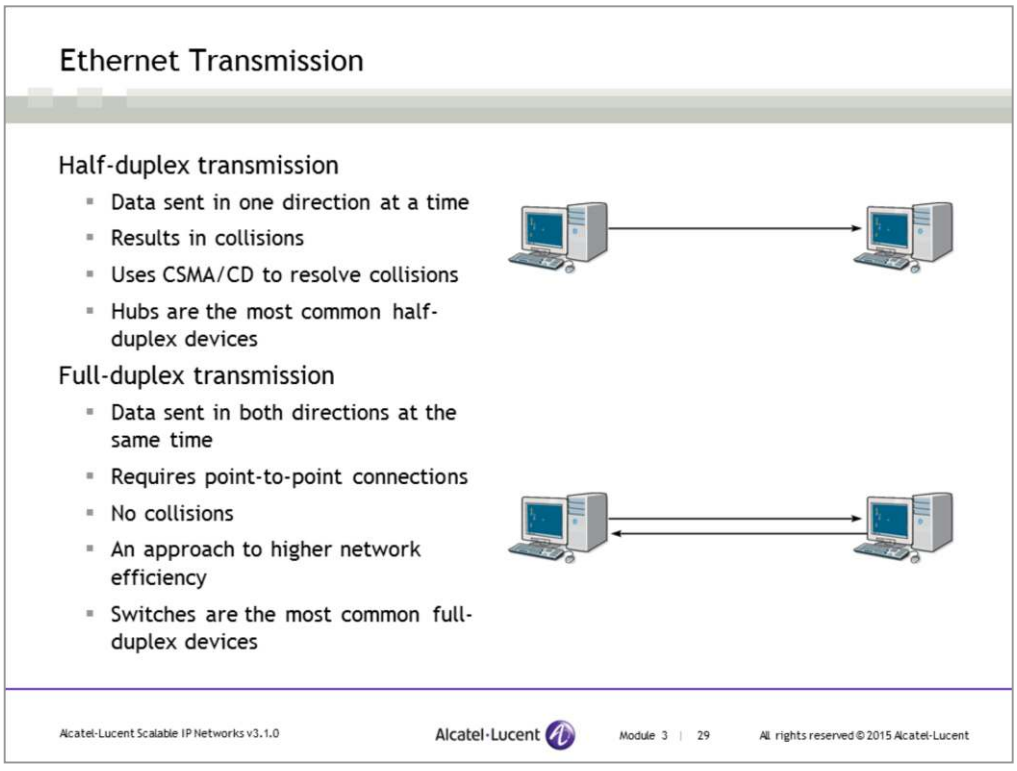
- 239.1.1.1=01-00-5E-01-01-01

For more information about conversion between the IP multicast address and the MAC address, please refer to the SRC multicast course.

The frame is sent to a switch that connects all four devices. Assume the switch knows which device belongs to a particular multicast group. The switch sends the frame out to the appropriate ports. Only the devices that are members of the particular group (239.1.1.1) process the message.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Ethernet is a shared medium, meaning that many hosts share access to the same media. It is possible for more than one host to attempt to send information on the physical media at the same time. This is equivalent to two or more people on a conference call trying to speak at the same time.

A set of procedures or protocols are used that allow each Ethernet-attached station to gain access to the shared media when the station needs it, but that prevents any one station from monopolizing the conversation.

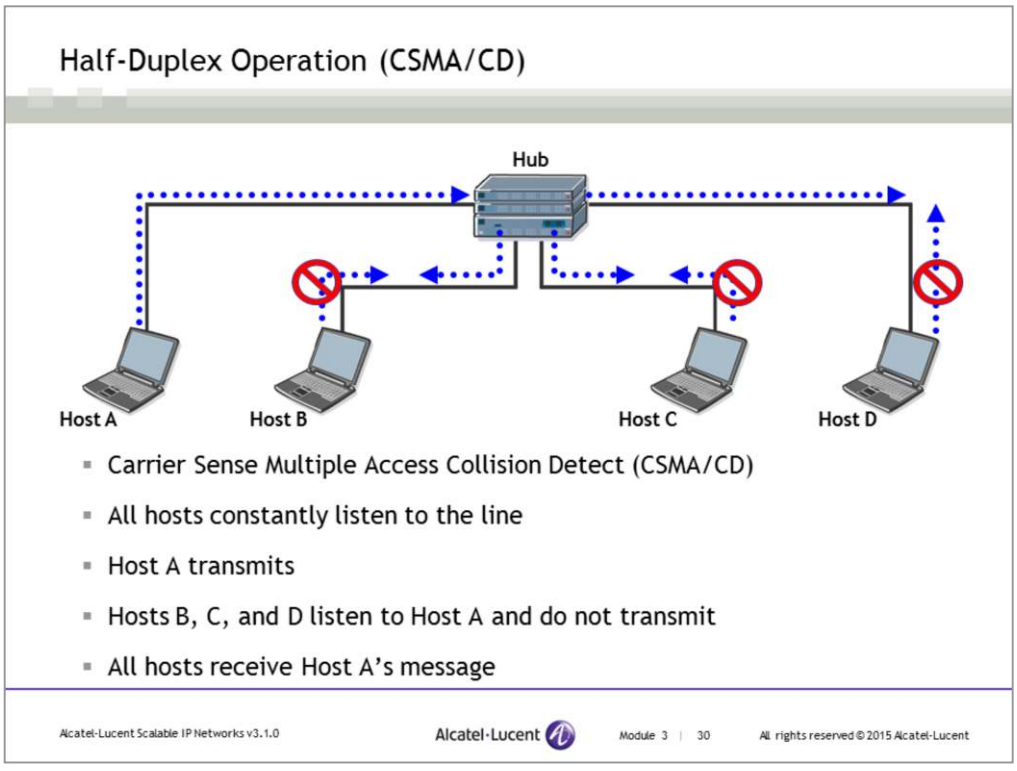
Half-duplex transmission is the traditional means of transporting Ethernet frames. Because data is transmitted in one direction at a time over a shared medium, such as a hub, collisions are possible. The CSMA/CD algorithm is used to handle collisions. A hub uses shared media and supports half-duplex only. 10Base-T, which works on half-duplex, is efficient 30% to 40% of the time because of collisions, and as such the effective throughput is only 3 to 4 Mbps.

Full-duplex transmission has data forwarding in both directions simultaneously. Full-duplex implementations require a point-to-point connection between the sender and the receiver port. This ensures that there is no shared medium, no collisions, and no need to schedule retransmissions. Because data can be transmitted bi-directionally, the effective rate of a 10-Mbps, full-duplex transmission is 20 Mbps (10 Mbps each way). Therefore, full-duplex transmissions are more efficient than half-duplex. Switches and routers usually support full-duplex transmissions.

When devices such as switches and hubs are interconnected, care must be taken to ensure that the proper transmission parameters are set on the ports. For switch-to-hub connections, the switch port must be set to half-duplex because the hub only supports half-duplex. For switch-to-switch, switch-to-host, or switch-to-router connections, full-duplex can be used.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The CSMA/CD access rules are summarized by the protocol acronym.

Carrier sense (CS)— Each Ethernet LAN-attached host continuously listens for traffic on the medium to determine when gaps between frame transmissions occur.

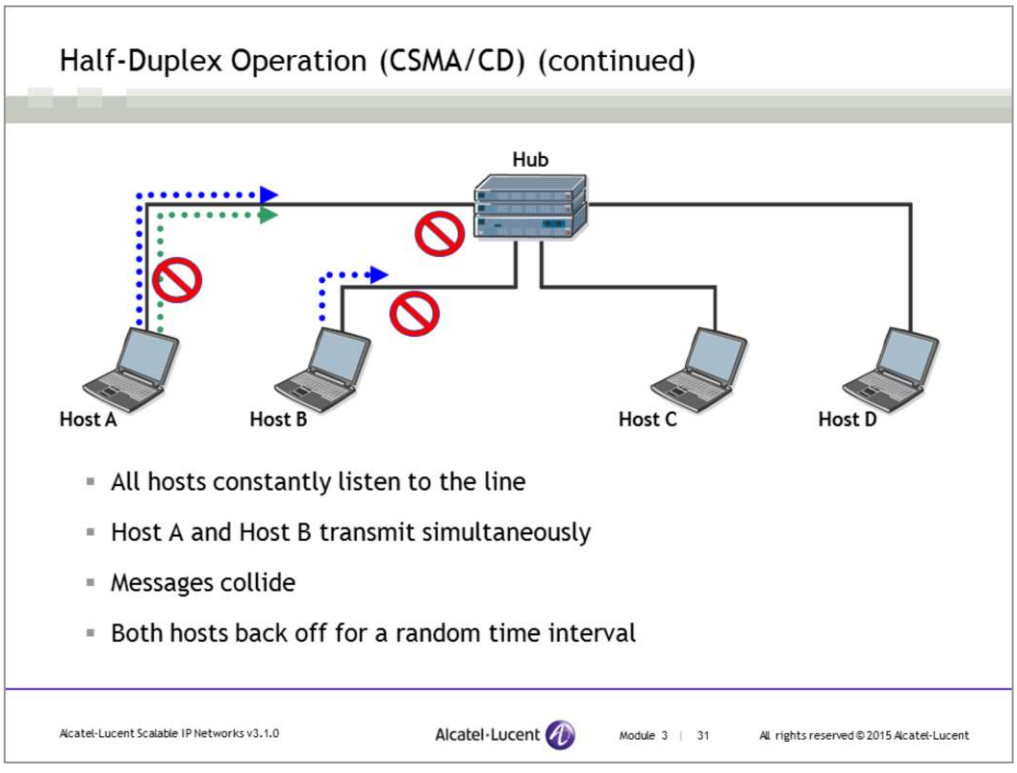
Multiple access (MA)— LAN-attached hosts can begin transmitting any time they detect the network is quiet, meaning that no traffic is travelling across the wire.

Collision detect (CD)— If two or more LAN-attached hosts in the same CSMA/CD network or collision domain begin transmitting at approximately the same time, the bit streams from the transmitting hosts will interfere (collide) with each other, and both transmissions will be unreadable. If that happens, each transmitting host must be capable of detecting that a collision has occurred before it has finished sending its respective frame. Each host must stop transmitting as soon as it has detected the collision and must wait a random length of time as determined by a back-off algorithm before attempting to retransmit the frame. In this event, each transmitting host transmits a 32-bit jam signal alerting all LAN-attached hosts of a collision before running the back-off algorithm.

The CSMA/CD reduces the chance of collisions but does not prevent them. Both hosts A and B could decide to transmit at once because no other hosts are transmitting a message on the line (idle line).

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



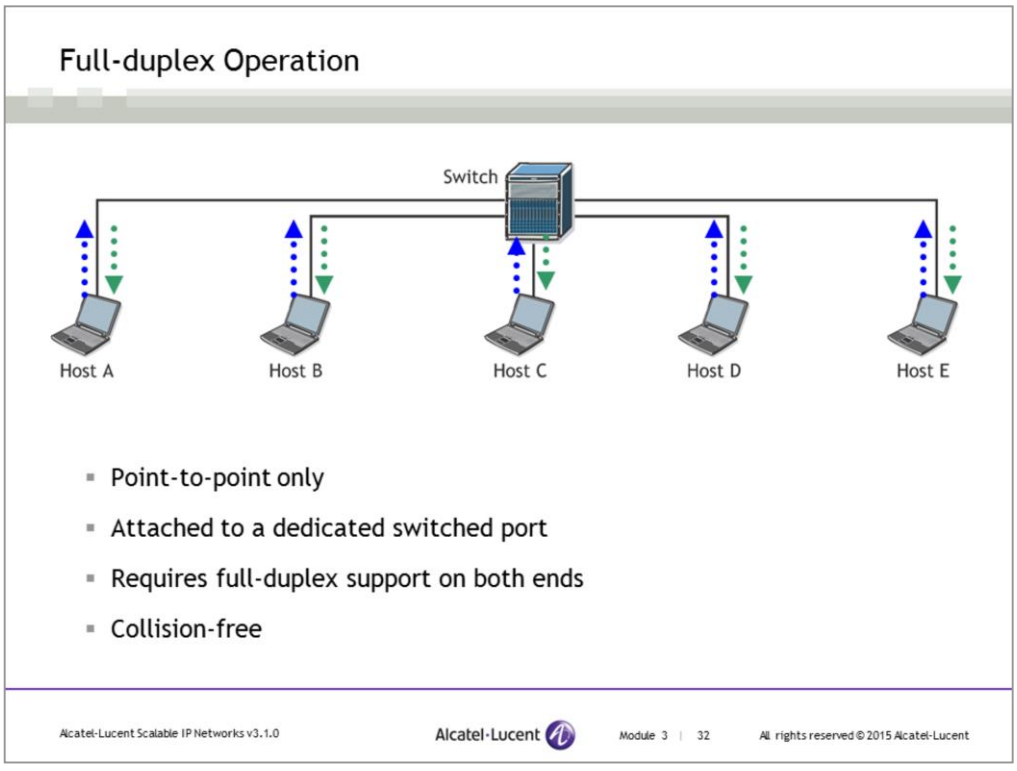
When host A and host B transmit frames at the same time, they both detect collisions and corruption of the data.

Both host A and host B generate a jam signal, which is received by other hosts so that they discard the data that was just corrupted by the collision.

A random back-off timer is then started on the transmitting hosts. Depending on whose timer expires first, either host A or host B transmits if they detect no other transmission on the line.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



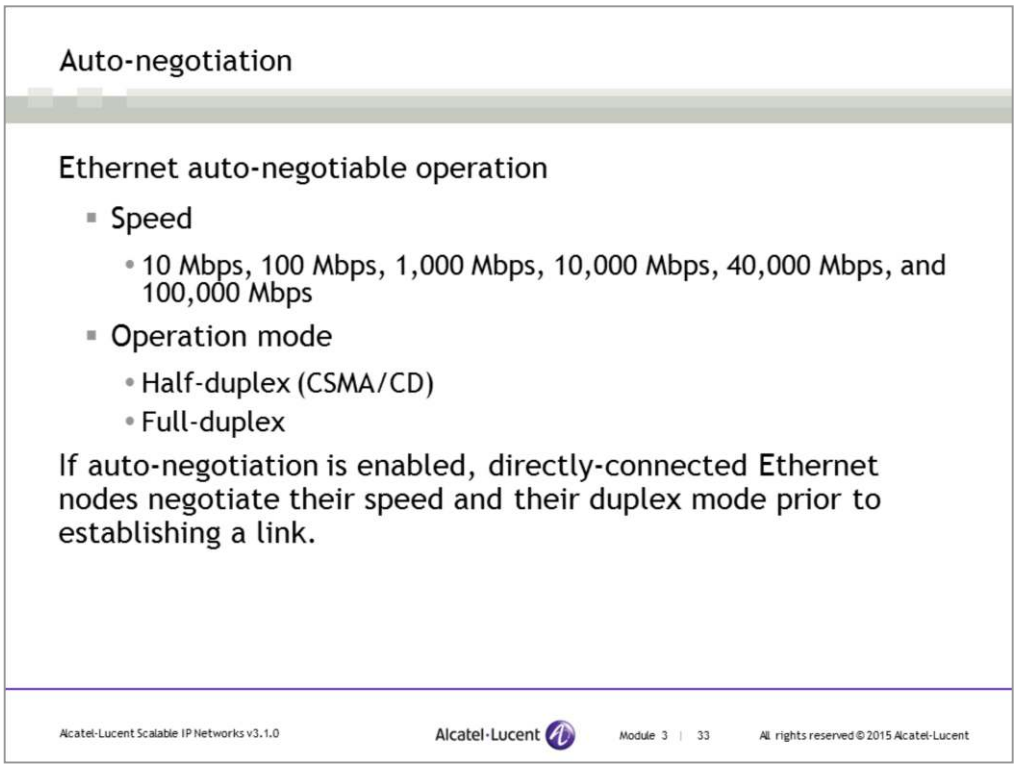
Full-duplex operation is an optional MAC layer capability that allows simultaneous two-way transmission over point-to-point links.

Full-duplex transmission involves no media contention, no collisions, and no need to schedule retransmissions. There are exactly two hosts connected on a full-duplex point-to-point link.

The link bandwidth is effectively doubled because each link can now support full-rate, simultaneous, two-way transmission.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

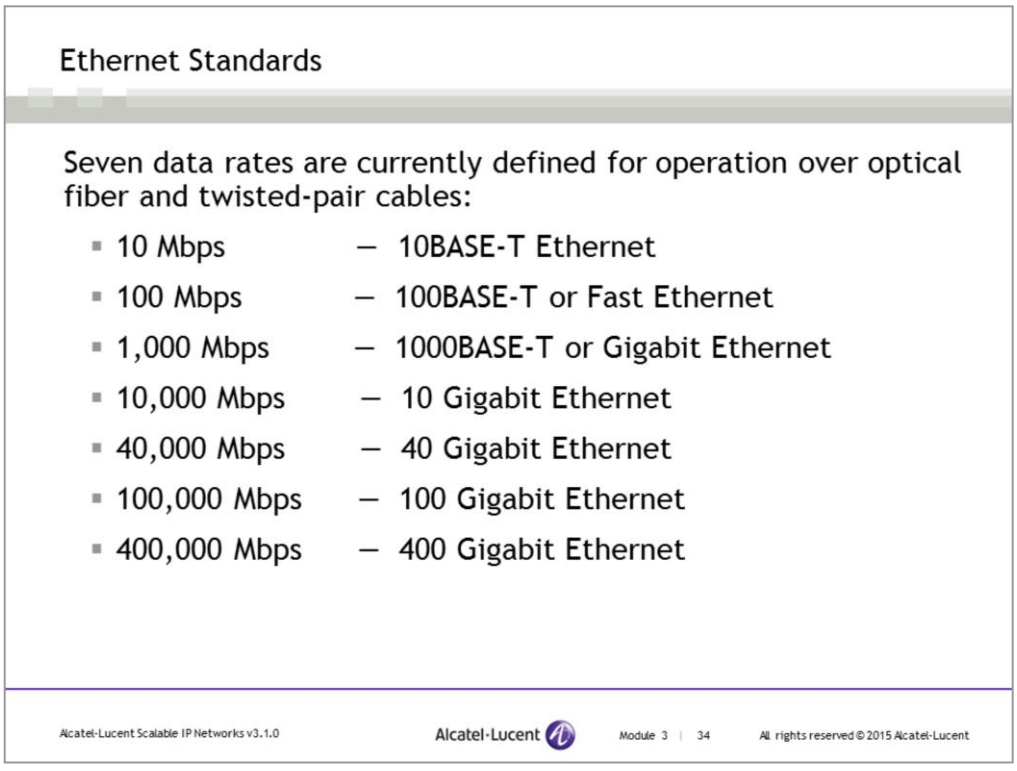


If auto-negotiation is enabled, directly-connected Ethernet nodes negotiate their speed as well as duplex mode prior to establishing a link. In theory, you could allow all Ethernet devices to auto-negotiate their speed and duplex mode. In practice, however, it is much better to manually set the speeds and modes of your devices to ensure that all of your Ethernet devices are operating at the speeds and modes you expect. Many network problems have been traced to a simple mismatch between speed or duplex mode on neighboring devices, so it is best practice to make certain that this situation does not arise in your network.

Note that not all Ethernet speeds support half-duplex operation. For example, 10,000 Mbps or 10 GigE does not support half-duplex operation.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Modern Ethernet takes advantage of enhanced data rates and distances through the use of twisted-pair and fiber optical cabling. This slide shows a list of standards currently defined.

The leading number of BASE-T refers to the transmission speed in Mbps. BASE refers to baseband digital transmission. The T refers to the twisted pair cable.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

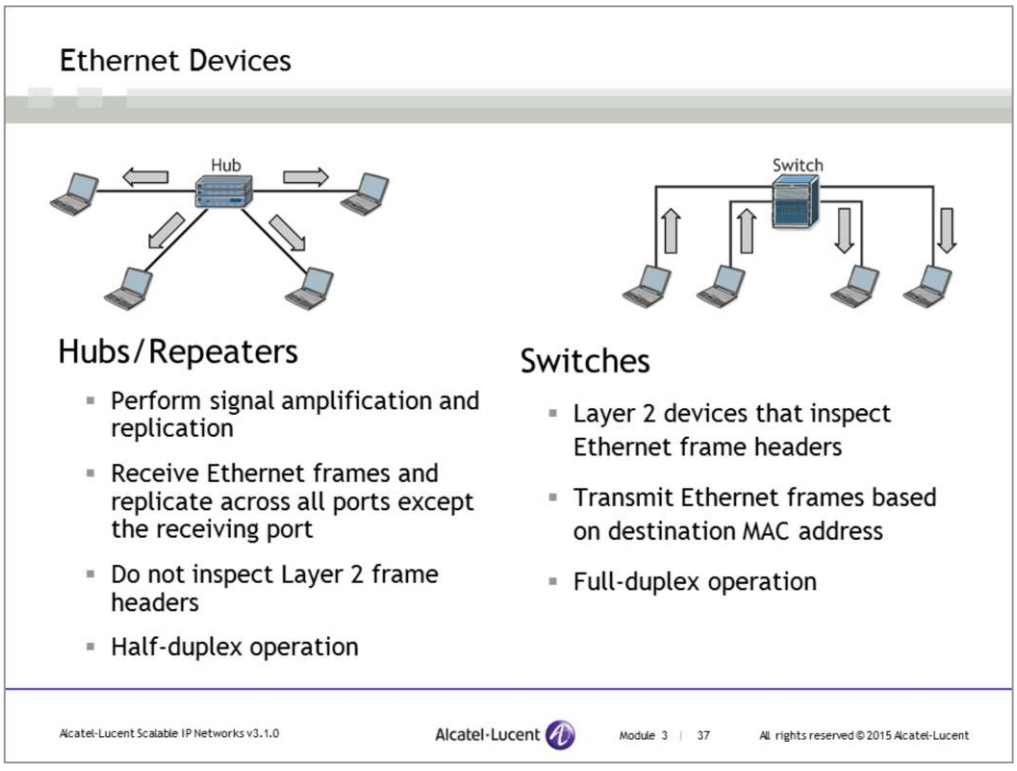
After successful completion of this section, you will be able to:

- Compare the functions of a hub and a switch
- Explain the purpose of the MAC forwarding database and how it is populated
- Describe how a switch forwards unicast, multicast, and broadcast frames
- Describe the properties of collision domain and broadcast domain
- Identify collision domains and broadcast domains given a network topology with Ethernet devices

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 3 | 36
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



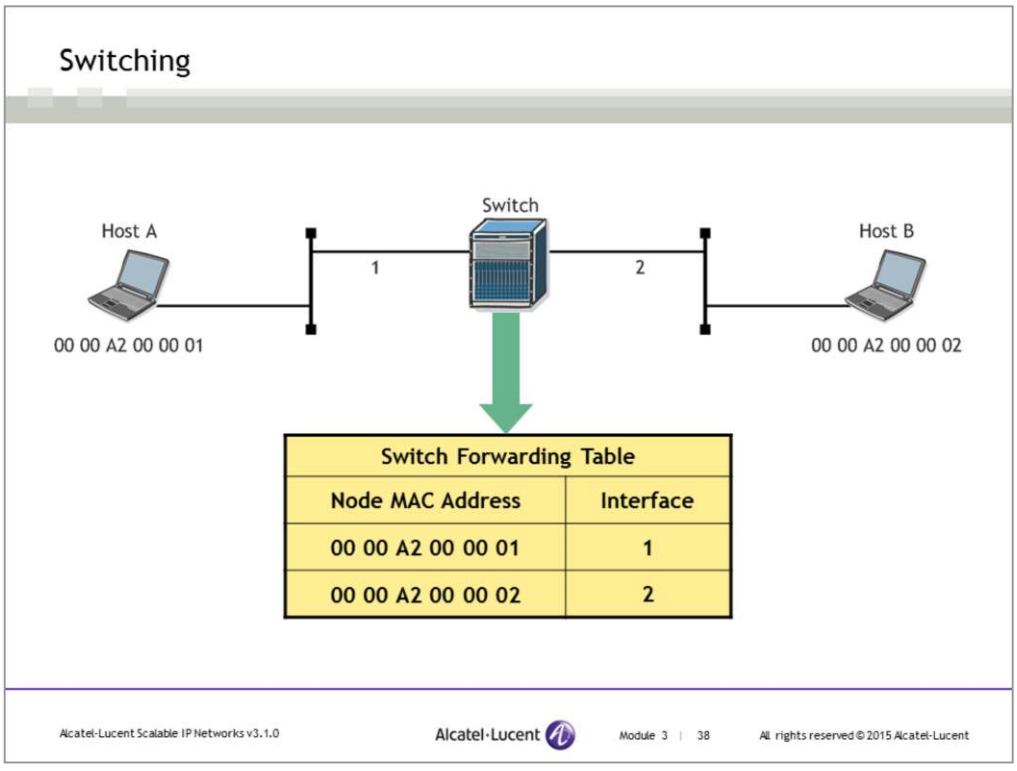
A repeater is used to repeat an Ethernet signal along a wire. In modern networks, repeaters are rarely used or needed and are mentioned here only for historical purposes.

An **Ethernet hub** is a device that connects Ethernet devices so that they can communicate with each other. Any Ethernet frame that arrives on any port is automatically forwarded to every other port. Any device on a hub can talk to any other device on a hub and, indeed, there is no way to prevent this from happening. A hub provides no intelligent filtering or forwarding capabilities at all. An Ethernet hub simply mimics the functions of an Ethernet wire. It is half-duplex only, so collisions can occur.

Similar to an Ethernet hub, an **Ethernet switch** is also a device that connects Ethernet devices so that they can communicate with each other. An Ethernet switch can forward an Ethernet frame only to a certain port or ports that actually need it. A switch can also provide full-duplex capabilities and therefore avoid collision. A switch processes the Ethernet header information in the frame and determine what the destination MAC address is. It will then make an intelligent forwarding decision and send the frame only to the port that needs to receive that destination MAC address. Also, switches provide more intelligence to buffer frames and prevent collisions on the backplane, enabling full-duplex conversations.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Ethernet switches use the source MAC address to dynamically learn which MAC addresses are associated with an interface. The switch records this address information into a forwarding table known as the MAC forwarding database (FDB).

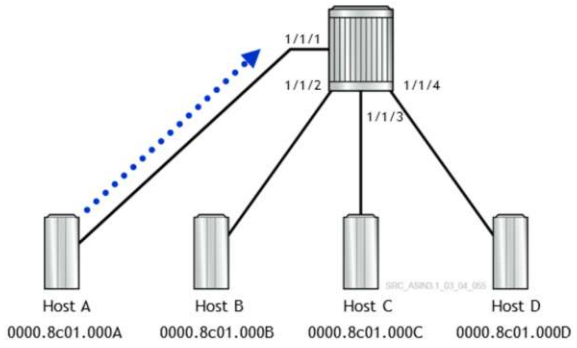
When the switch receives an Ethernet frame, it records the source MAC address and the interface on which it arrived. It looks at the destination MAC address of the frame, compares it to the entries in its MAC FDB, and transmits the frame out of the interface for that MAC address.

If no entry is found in the MAC FDB for the destination, the switch floods the frame out of all its interfaces, except the interface on which the frame arrived. If the destination device responds, the switch will learn the MAC address on the receiving port, and future flooding for that destination will be unnecessary.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB



MAC FDB

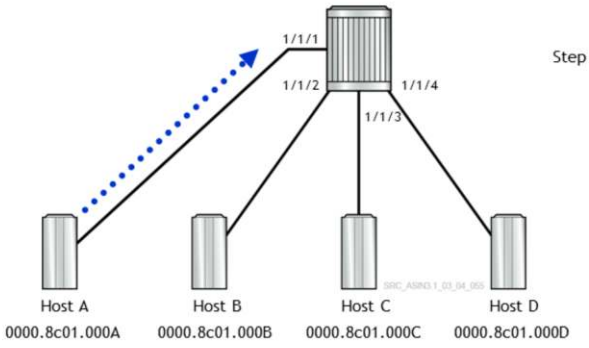
1/1/1	
1/1/2	
1/1/3	
1/1/4	

Step 1: Host A sends a frame to Host B

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB (con't)



MAC FDB

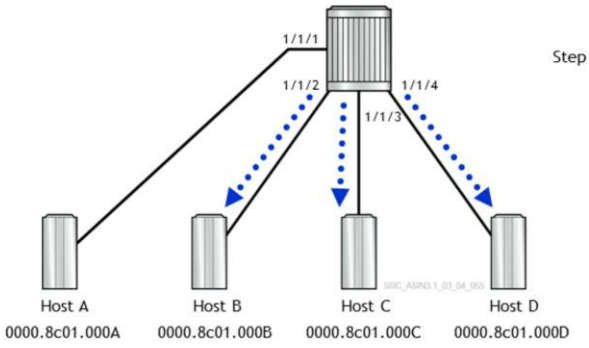
Step 2		
	1/1/1	0000.8c01.000A
	1/1/2	
	1/1/3	
	1/1/4	

Step 2: The switch receives the frame on 1/1/1 and places the source in MAC FDB

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB (con't)



MAC FDB

Step 2

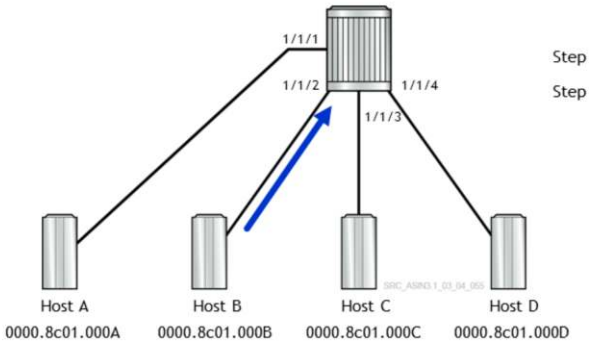
1/1/1	0000.8c01.000A
1/1/2	
1/1/3	
1/1/4	

Step 3: The destination is not in the MAC FDB, so the switch floods the frame to all ports except the source

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB (con't)



MAC FDB

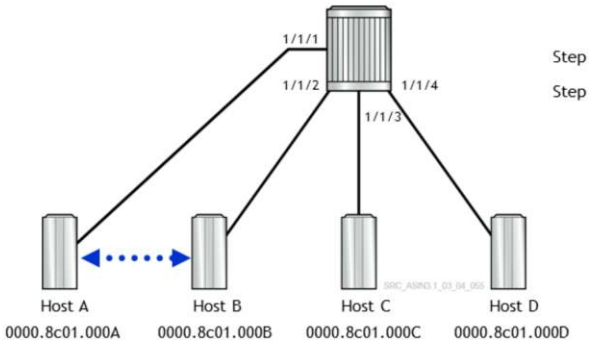
Step 2	1/1/1	0000.8c01.000A
Step 4	1/1/2	0000.8c01.000B
	1/1/3	
	1/1/4	

Step 4: Host B responds to Host A. The switch adds the source address of Host B to the MAC FDB

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB (con't)



MAC FDB

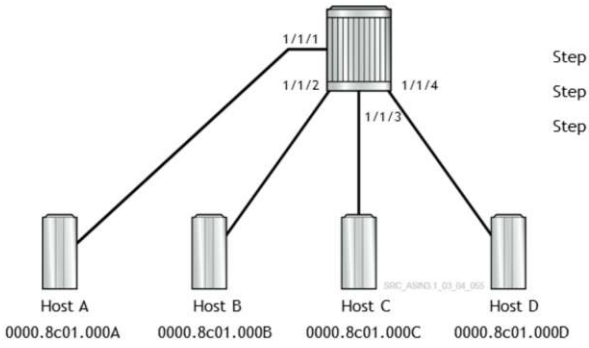
Step 2	1/1/1	0000.8c01.000A
Step 4	1/1/2	0000.8c01.000B
	1/1/3	
	1/1/4	

Step 5: The switch can now forward frames between Host A and Host B directly without flooding

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Building up the MAC FDB (con't)



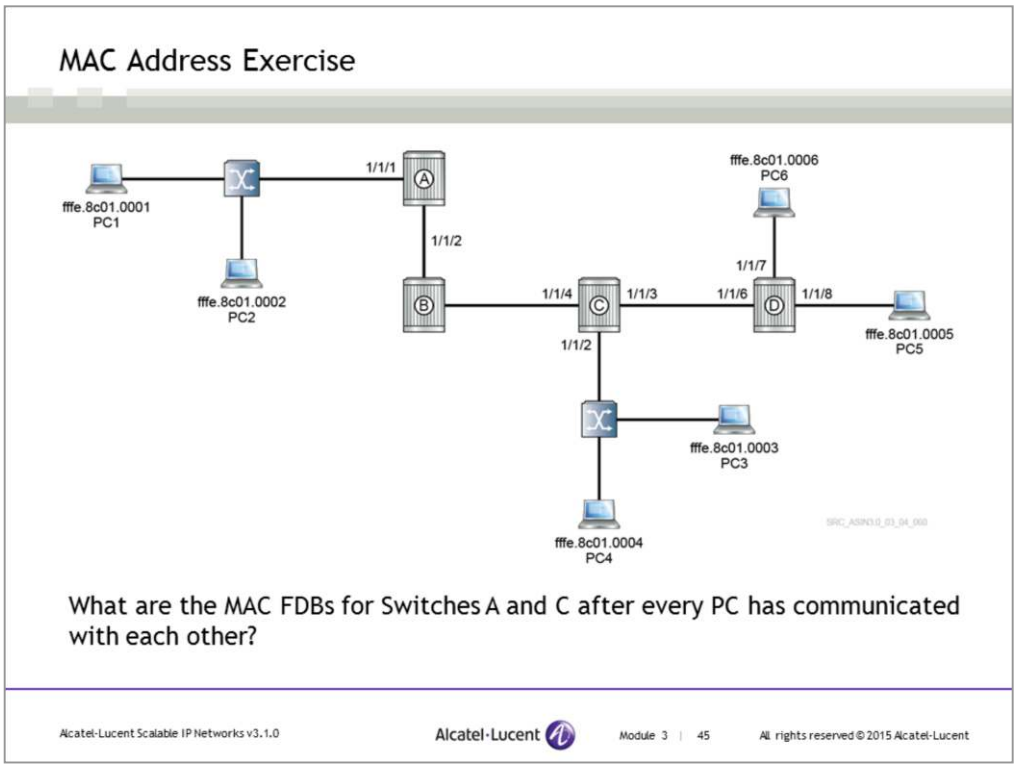
MAC FDB

Step 2	1/1/1	0000.8c01.000A
Step 4	1/1/2	0000.8c01.000B
Step 6	1/1/3	0000.8c01.000C
	1/1/4	0000.8c01.000D

Step 6: Host C and Host D also send frames and added to the FDB

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



After every PC has communicated with each other, the following entries will be shown in Switch A's MAC FDB and Switch C's MAC FDB.

Switch A's MAC FDB:

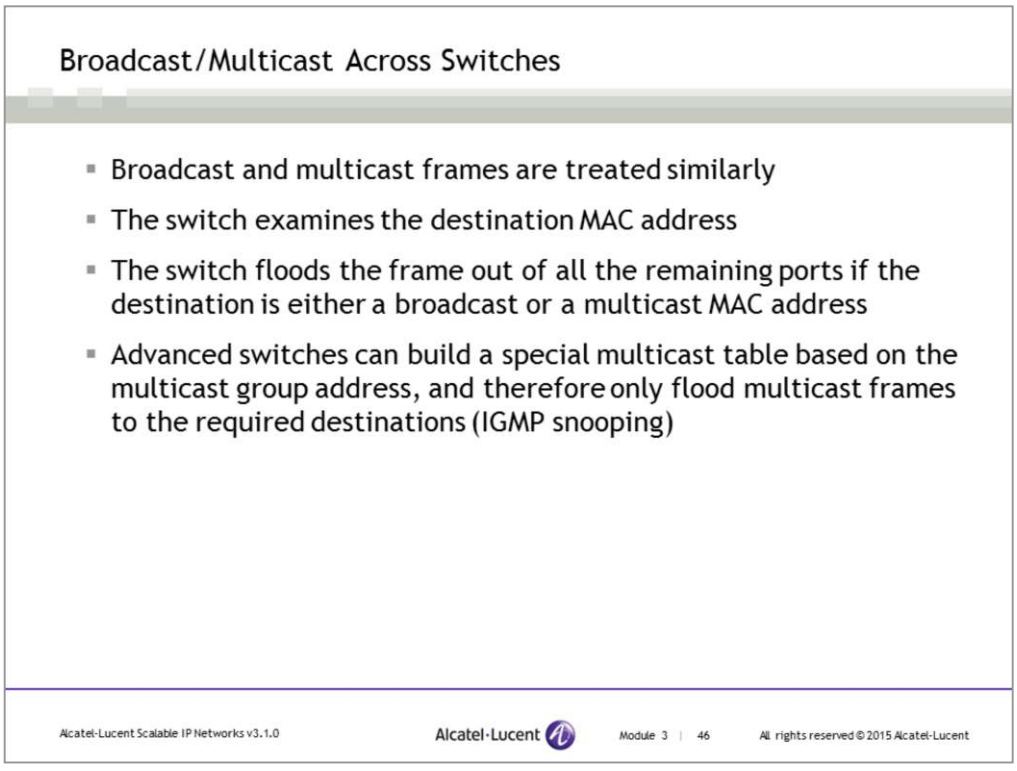
Interface	**MAC address**
1/1/1	fffe.8c01.0001
1/1/1	fffe.8c01.0002
1/1/2	fffe.8c01.0003
1/1/2	fffe.8c01.0004
1/1/2	fffe.8c01.0005
1/1/2	fffe.8c01.0006

Switch C's MAC FDB:

Interface	**MAC address**
1/1/4	fffe.8c01.0001
1/1/4	fffe.8c01.0002
1/1/2	fffe.8c01.0003
1/1/2	fffe.8c01.0004
1/1/3	fffe.8c01.0005
1/1/3	fffe.8c01.0006

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

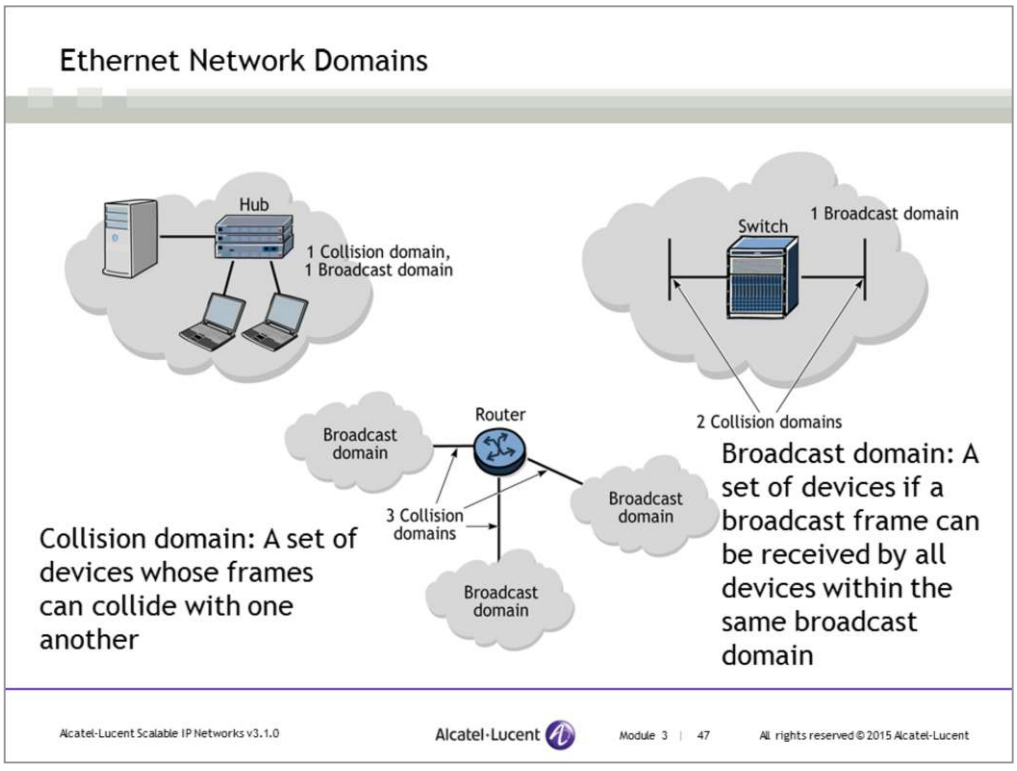


A unicast Ethernet frames are intended for a single destination, there are also broadcast frames intended for all devices and multicast frames intended for groups of devices.

Normally, both types of frames are treated the same. They are flooded out of every port except the port it was received on. In other words, they are treated the same way as a unicast frame with a destination MAC that is not in the FDB. There are advanced switches that will also build special multicast FDB tables based on the multicast group destination address and will therefore only flood multicast frames to the destinations that belong to the specified multicast group. The process of building the special multicast table is called IGMP snooping. Please consult Alcatel-Lucent SRC multicast course for details about IGMP snooping.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A **collision domain** is a group of Ethernet or Fast Ethernet devices in a CSMA/CD LAN that are connected by repeaters and that compete for access in the network. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network to avoid data collisions. A collision domain is sometimes referred to as an Ethernet segment. Every port on an Ethernet switch is considered a single collision domain.

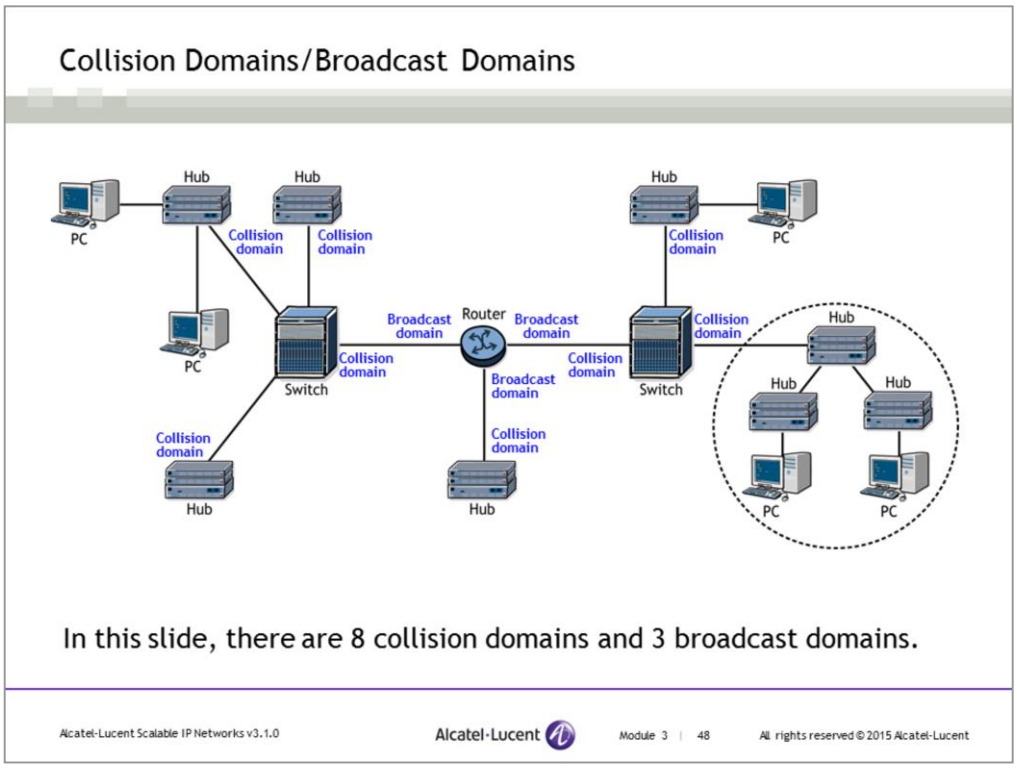
A **broadcast domain** is a restricted area in which information can be transmitted to all devices in the domain. More specifically, Ethernet LANs are broadcast domains. Any device attached to the LAN can transmit frames to any other device because the medium is a shared transmission system. Frames are normally addressed to a specific destination device in the network. While all devices detect the frame transmission in the network, only the device to which the frame is addressed actually accepts it. Within a broadcast domain, every Ethernet device will receive and process all broadcast packets.

In an IP network, broadcast domains are separated by an IP router. Two devices on separate broadcast domains cannot send Ethernet frames directly to each other. Instead they must send the frame to the router which then forwards the IP datagram to the destination in a new Ethernet frame on the appropriate broadcast domain.

Hubs provide no separation for collision or broadcast domains, switches provide collision domain separation, and routers provide both collision and broadcast domain separation.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

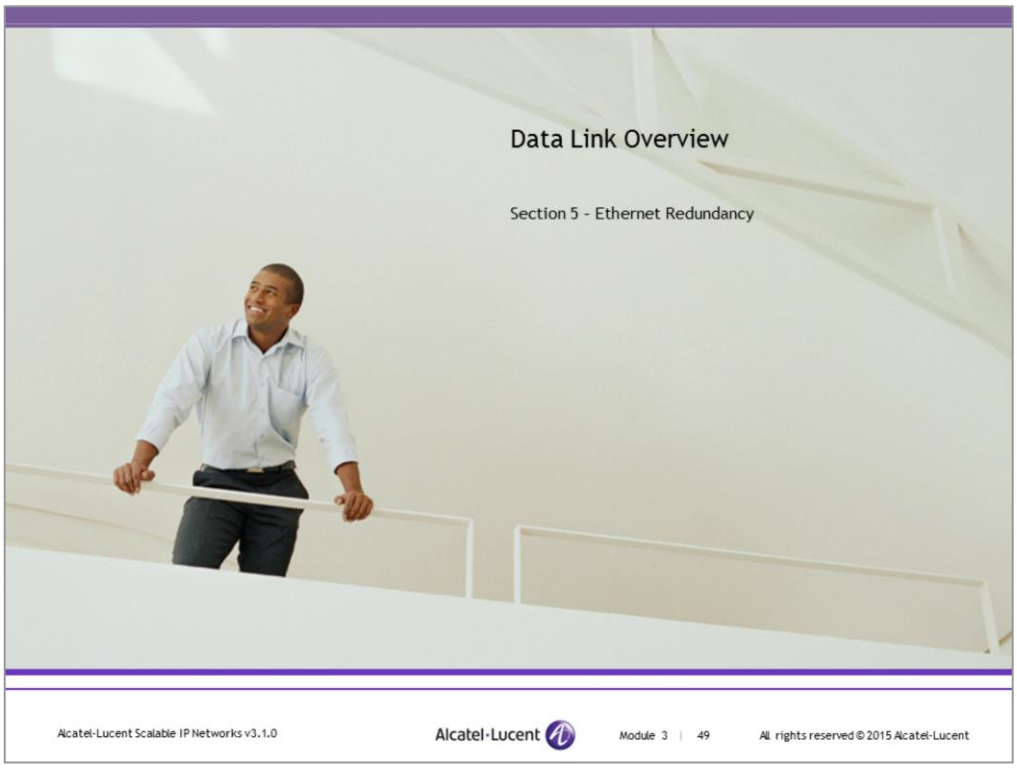


Routers operate at Layer 3, so an Ethernet frame would not be forwarded across a router. The boundary or domain that includes all of the Ethernet switches contained by a router boundary is a broadcast domain. In this slide, there is one router and the router is connected to two switches and one hub. In total, there are 3 broadcast domains.

A collision domain is a physical segment where data packets can collide with one another on a shared media. A hub itself is an entire collision domain. Also, each port on a switch is a collision domain. In the switch on the left, there are four ports connecting to devices. In the switch on the right, there are three ports connecting to devices. In total, there are eight collision domains.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

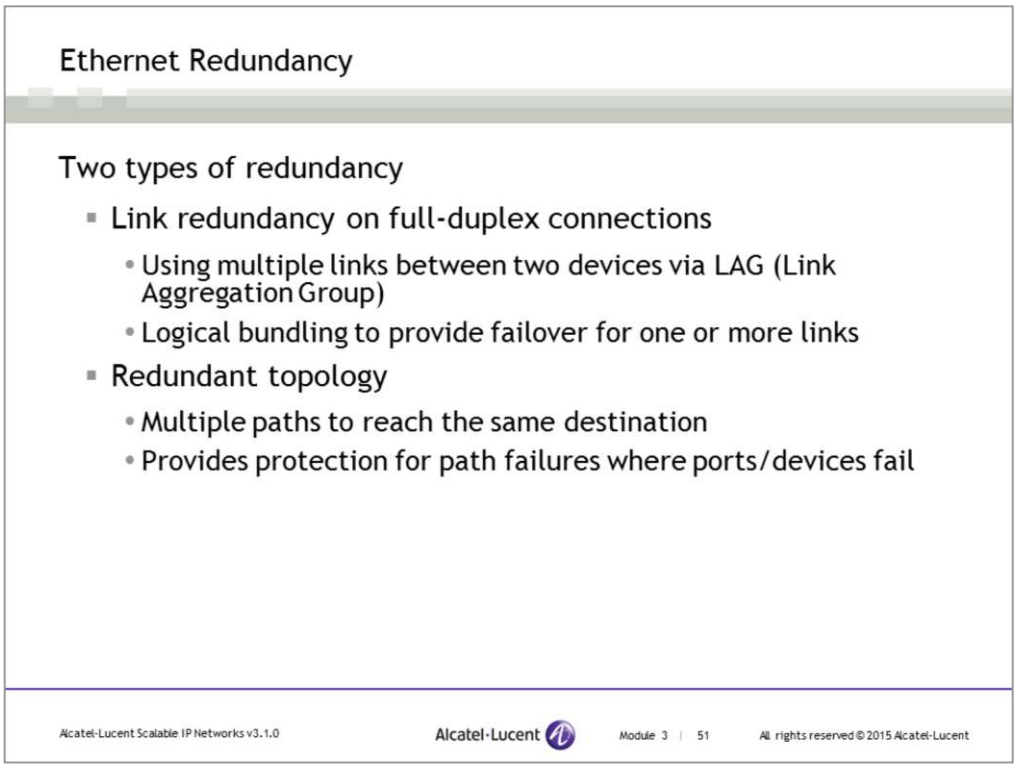
After successful completion of this section, you will be able to:

- Describe two types of Ethernet redundancy: LAG and STP
- Calculate the cost of LAG based on the number of links, dynamic-cost and port-threshold
- Configure a static LAG group
- Explain the requirements for using STP
- Describe the functions of STP

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 3 | 50
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

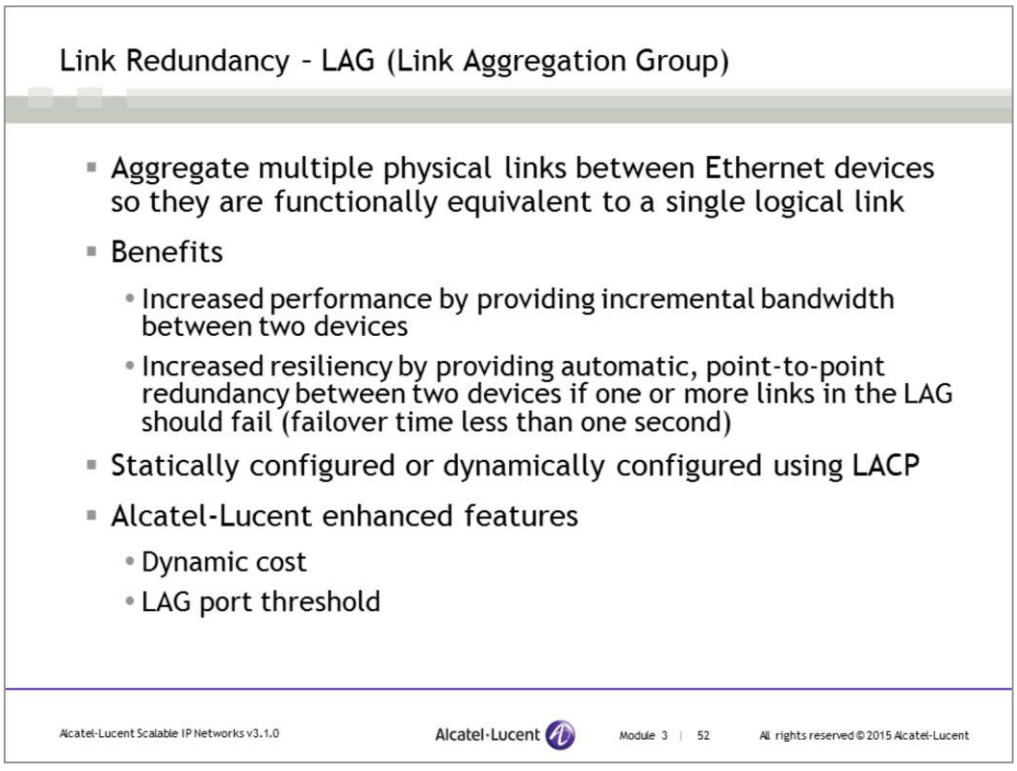


It is good design practice to provide redundancy in the event of failure. There are two basic types of redundancy available with Ethernet networks: link redundancy and path redundancy. Link redundancy is provided via the Link Aggregation Group (LAG) protocol. Path redundancy is provided by the Spanning Tree Protocol (STP).

The link redundancy does not provide redundancy in the event of a switch failure. For example, a failure of a single or of multiple links between LAG-connected switches would be survivable. However, there are sometimes failures of an entire switch. In this case, all available links on a particular path are lost, and full redundancy would be required.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Link Aggregation Control Protocol (LACP) is defined in IEEE 802.1AX and IEEE 802.1aq (Aggregation of Multiple Link Segments). LAG allows aggregating multiple physical links between Ethernet devices so that they are functionally equivalent to a single logical link. The standard specifies several important requirements for vendor implementations.

1) All links in a LAG group must be full-duplex and must have the same speed.

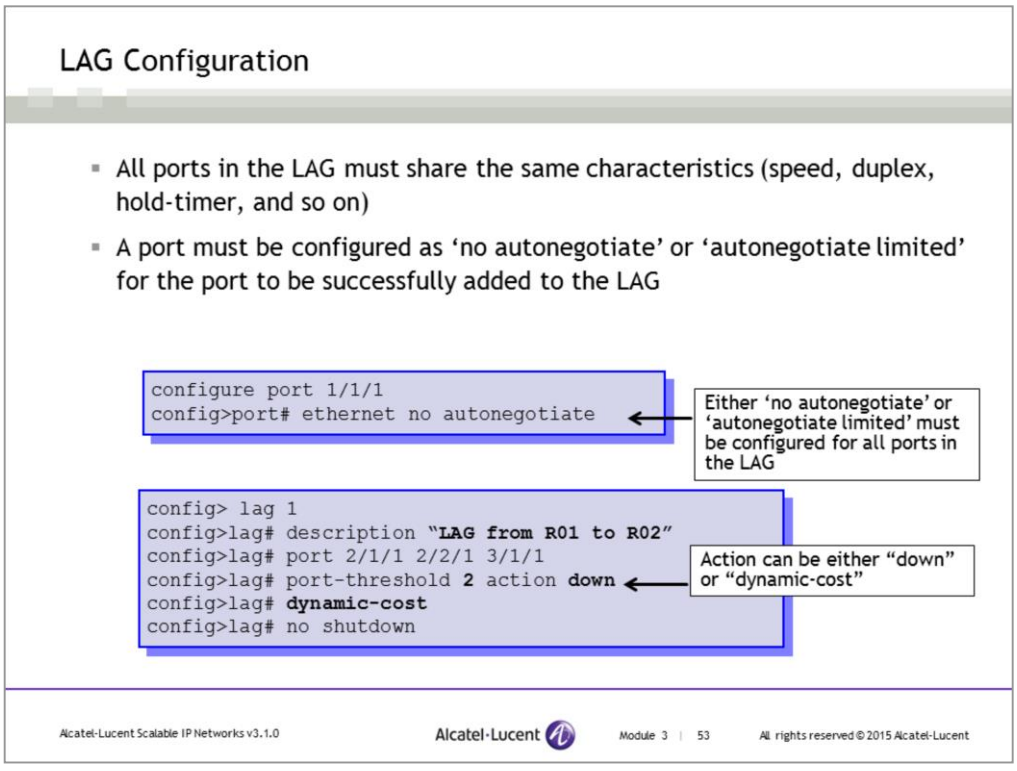
2) The LAG implementation must not reorder frames as they are transmitted across the LAG group. This means that all frames transmitted between the same source/destination MAC address pair will be transmitted across the same physical link in the bundle. The result is that some links in the bundle may have more traffic than others, so traffic may not be perfectly load-balanced across all links.

A Link Aggregation Group (LAG) increases the bandwidth available between two nodes by grouping multiple ports into one logical link. The aggregation of multiple physical links allows for load sharing and offers seamless redundancy. If one of the links fails, traffic is redistributed over the remaining links in less than 1 second.

LAG can be statically configured between devices, or it can be forced dynamically through the use of Link Aggregation Control Protocol (LACP). LACP provides a standardized method for implementing link aggregation among different manufacturers. The static configuration provides more control in the network with the expanses of increased management overhead. Using LACP reduces the need for configuration management but may result in unexpected LAG groups in the network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



LAG Port Threshold Parameter

This parameter determines the behaviour of a LAG when the number of available links falls below the configured threshold value. Two actions can be specified:

- **Option 1**:
  `configure lag <lag-id> port-threshold <threshold value> action` **`down`**
  If the number of available links is less than or equal to the threshold value, the LAG is declared operationally down until the number of available links is greater than the threshold value.
- **Option 2**:
  `configure lag <lag-id> port-threshold <threshold value> action` **`dynamic-cost`**
  If the number of available links is less than or equal to the threshold value, dynamic costing is used to determine the advertised LAG cost.
- **Note**: The costing of a LAG only affects the IGP costing (OSPF only)

Dynamic Cost Parameter

Dynamic cost can be enabled with the general command `config>lag <lag-id>` **`dynamic-cost`**.

This parameter enables or disables the dynamic IGP cost of a LAG when the number of active links is greater than the port-threshold value.

When dynamic cost is enabled with this command and the number of active links is greater than the port-threshold value, the path cost is dynamically calculated whenever there is change in the number of active links, regardless of the specified port-threshold action.

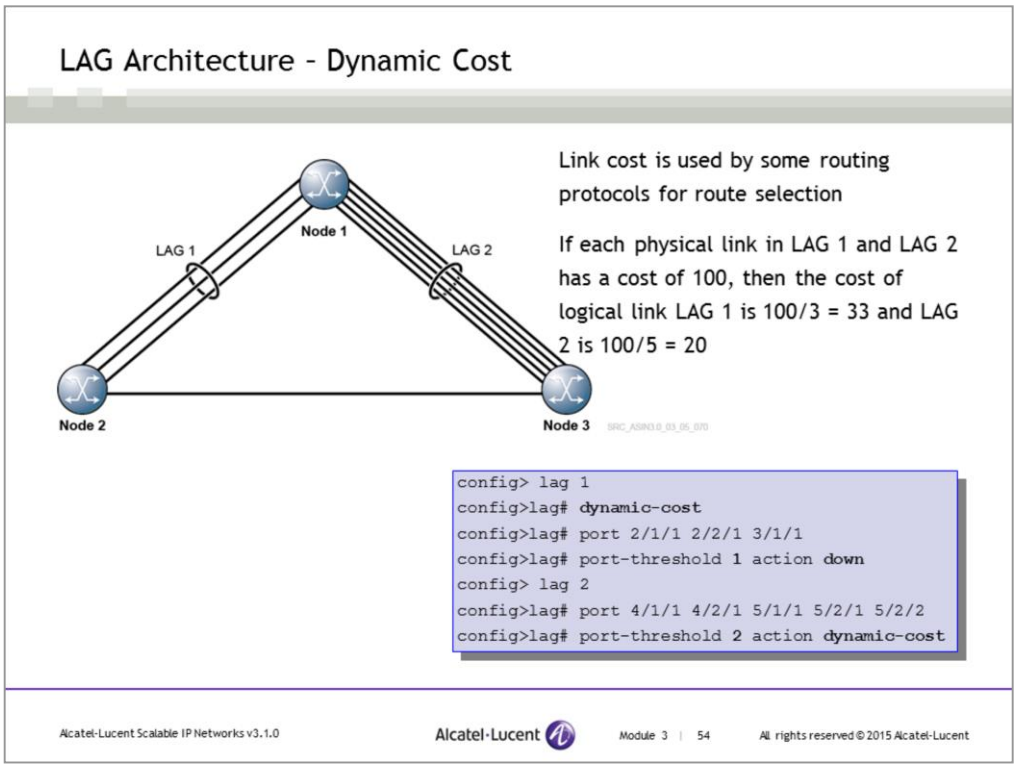
However, if the port-threshold action is configured as 'down' and the number of active links falls below the port-threshold, the LAG is declared down even if the general dynamic cost parameter is configured.

Conversely, if the port-threshold is met and the port-threshold action is configured as "dynamic cost", the link cost is dynamically recalculated even if the general dynamic cost parameter is not configured.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



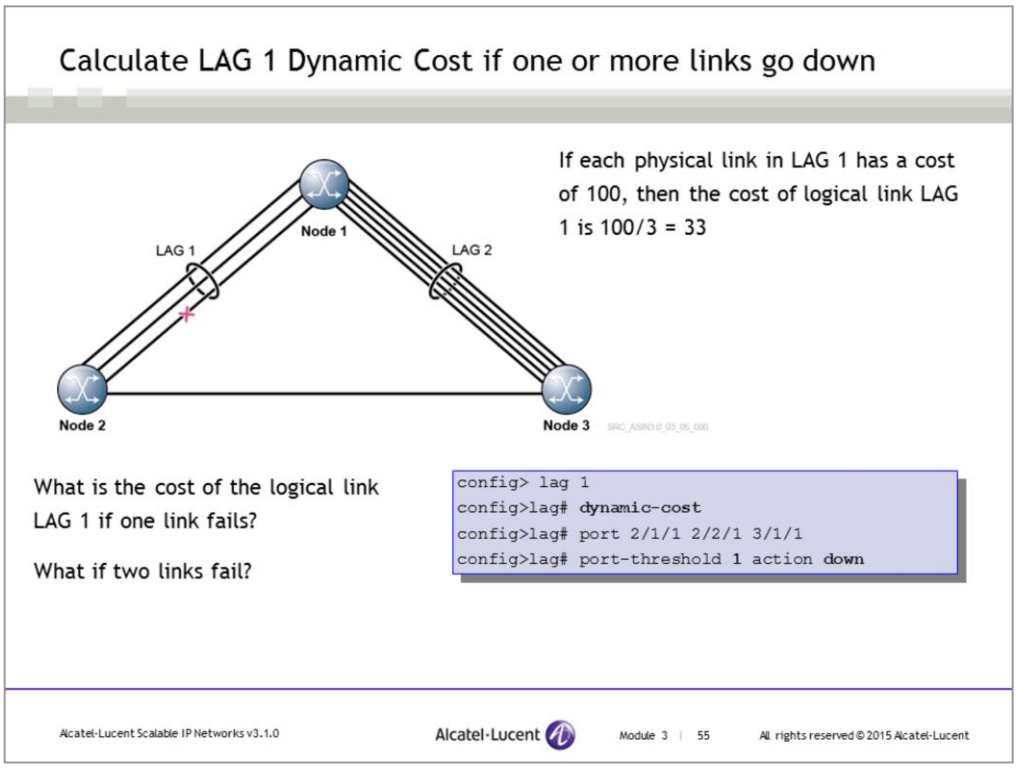
Link cost is used by some routing protocols (link state protocols such as OSPF and ISIS) to select the best path to a destination.

In this slide, each physical link is configured with a cost of 100. Thus, the cost of the logical link LAG 1 is 100/3 = 33 and LAG 2 is 100/5 = 20.

Overall, LAG is a good solution for providing link redundancy between neighbouring Ethernet devices. However, if end-to-end path redundancy is required, LAG cannot provide this functionality.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



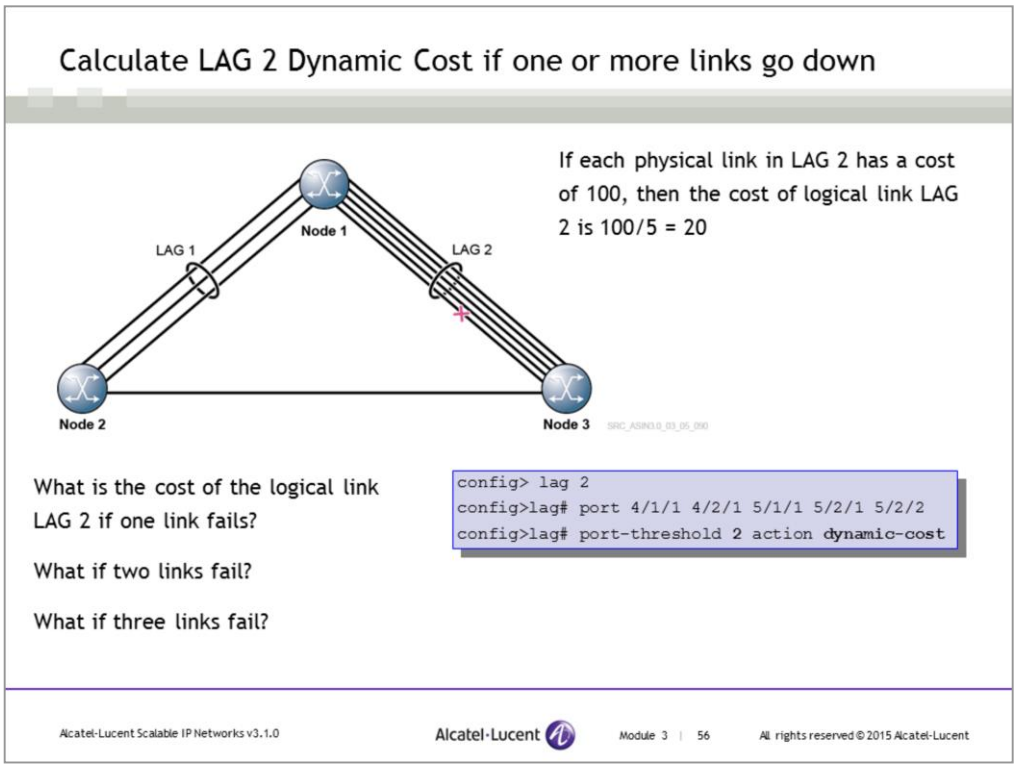
In this slide, each physical link is configured with a cost of 100. Thus, the cost of the logical link LAG 1 is 100/3 = 33. One of the link on LAG 1 fails.

LAG 1 has the dynamic-cost parameter configured. When one of the links in LAG 1 fails, there are still two active links. Since the port threshold is one, the port-threshold action is not executed. However, since the dynamic-cost parameter is enabled on the LAG, the cost of LAG 1 is dynamically calculated as 100/2 = 50.

If another link in LAG 1 fails, this leaves one active link. The number of active links matches the port threshold and the port-threshold action is executed, therefore LAG 1 is declared operationally down.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, each physical link is configured with a cost of 100. Thus, the cost of the logical link LAG 2 is 100/5 = 20. One of the link on LAG 2 fails.

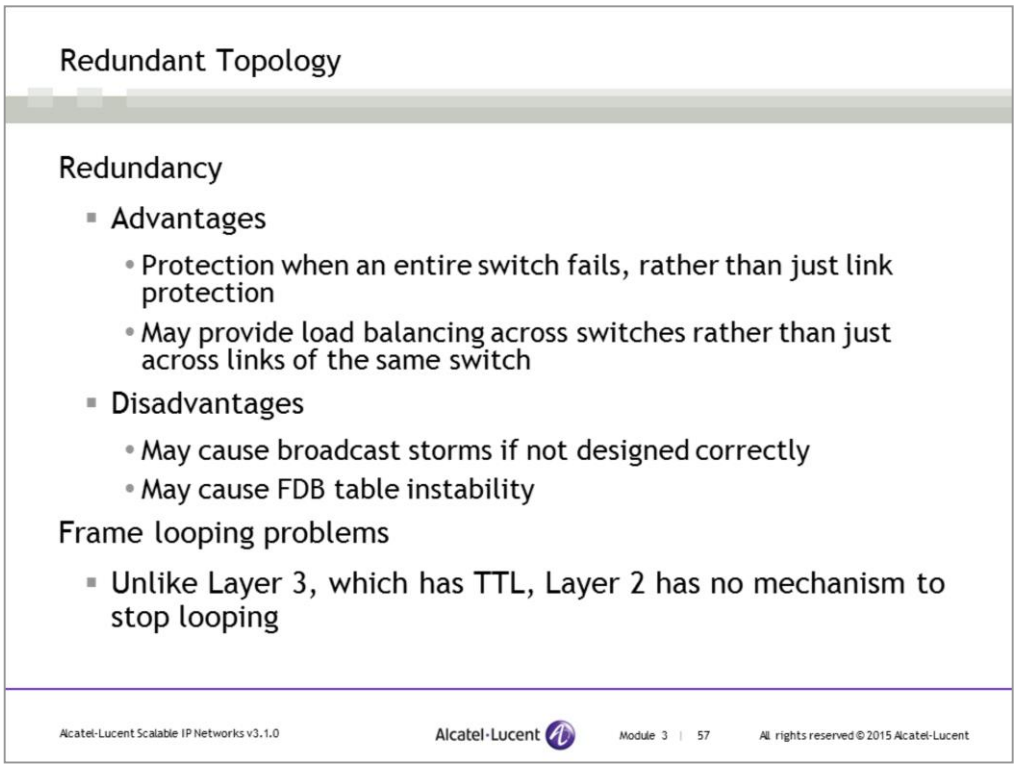
LAG 2 does not have the dynamic-cost parameter configured on the LAG. However, if one link in LAG 2 fails, there are four active links and the port threshold is two, so the port-threshold action is not executed. Since the dynamic-cost option is not enabled on the lag, the cost of LAG 2 remains as 100/5 = 20.

If a second link in LAG 2 fails, there are three active links and the port threshold is two, so the port-threshold action is not executed. Since the dynamic-cost option is not enabled on the lag, the cost of LAG 2 remains 100/5 = 20.

If a third link in LAG 2 fails, there are two active links. The number of active links matches the port-threshold, so the port-threshold action is executed. Therefore, the cost of LAG 2 is dynamically calculated as 100/2 = 50. LAG 2 is still operationally up unless there are no active links in the LAG.

All rights reserved © 2015 Alcatel-Lucent

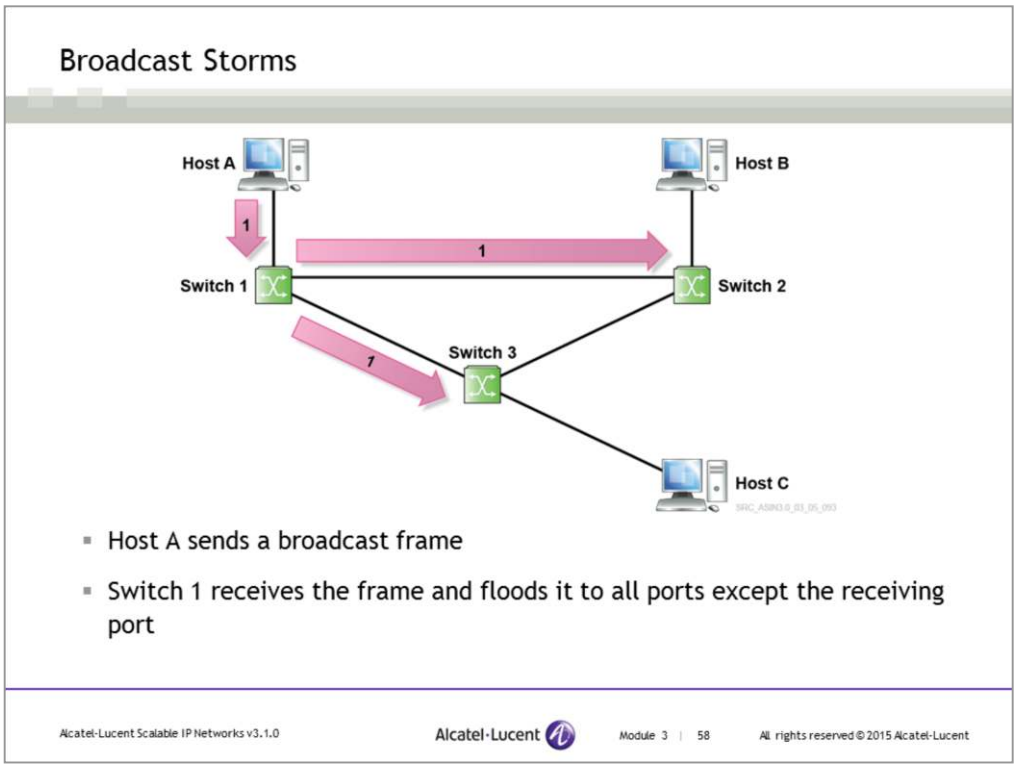
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Redundant topology provides an advantage over link redundancy by protecting the entire network in case a switch fails, and not just when individual links fail. However, there are some potential problems associated with providing path redundancy because of the nature of Ethernet switches. The disadvantages of redundant topology are broadcast storms caused by constant “looping” of Ethernet frames, and FDB table instability caused by switches that might see source addresses coming in on different interfaces.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A loop exists in a network when a frame or packet exits one interface on a device and then re-enters the device on a second interface. If the frame or packet returns again on the same second interface, the router or switch will again re-send the data back out of the original interface, and so forth and so on indefinitely. A router is a Layer 3 device and has a TTL (time to live) field that gets decremented when each router processes the packet. This prevents IP packets from existing forever on a network. No such field exist in an Ethernet device, so other mechanisms such as Spanning Tree Protocol (STP) must be employed.

Networks that are designed with redundancy and no Spanning Tree Protocol (STP) are vulnerable to broadcast storms because as the switch receives multiple copies of a frame, it further replicates each frame and transmits them out of one or more ports on the switch. Because of the Layer 2 loop, the transmitted frames are received back and replicated again. This results in an exponential increase in Layer 2 traffic in the looped network since this frame is copied and transmitted repeatedly until the switch gets overwhelmed with activity and possibly resets or locks up.

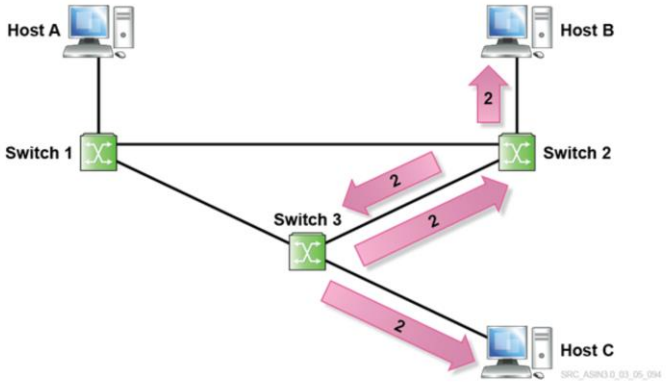
Consider the case where a host sends a broadcast frame:

1. Host A sends a broadcast frame to the Ethernet segment. Switch 1 receives the broadcast frame. Switch 1 replicates the broadcast frame and sends it out the port connected to Switch 2 and Switch 3.
2. Switch 2 and Switch 3 receive the frame from Switch 1. Switch 2 replicates the frame and sends it out the ports connected to Switch 3 and Host B. Similarly, Switch 3 replicates the frame and sends it out the ports connected to Switch 2 and Host C.
3. Switch 2 receives the frame from Switch 3 and replicates the frame and sends it out the ports connected to Switch 1 and Host B. Similarly, Switch 3 receives the frame from Switch 2 and replicates the frame and sends it out the ports connected to Switch 1 and Host C.
4. The process continues indefinitely as all three switches replicate the broadcast frame and send it out to all other ports except the receiving port, causing a broadcast storm.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Broadcast Storms (con't)

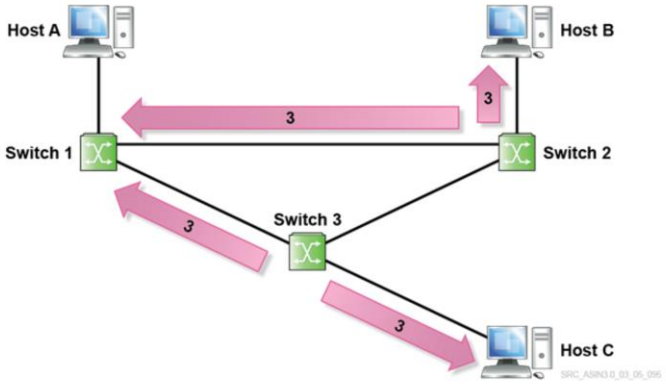


- Switch 2 receives the broadcast frame from Switch 3
- Switch 3 receives the broadcast frame from Switch 2
- Both switches flood the frame to all ports except the receiving ports

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Broadcast Storms (con't)

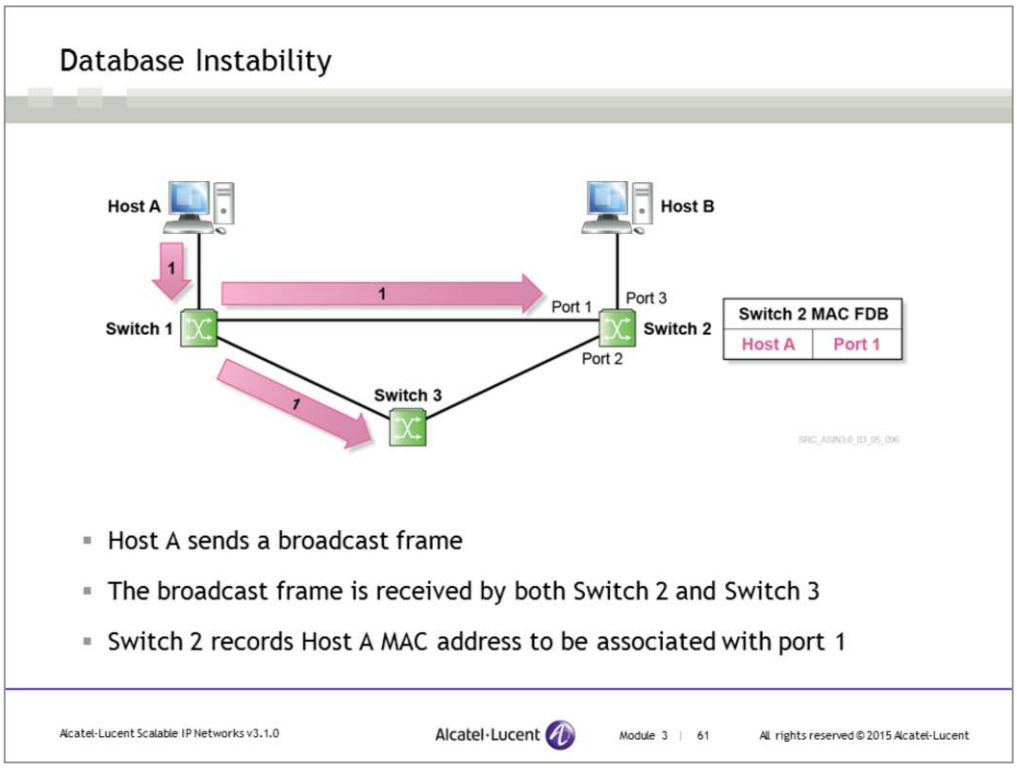


- Switch 2 and Switch 3 receive the broadcast frame from Switch 1
- Both switches flood the frame to all ports except the receiving ports
- The process continues indefinitely causing broadcast storm and consumes all switch resources

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

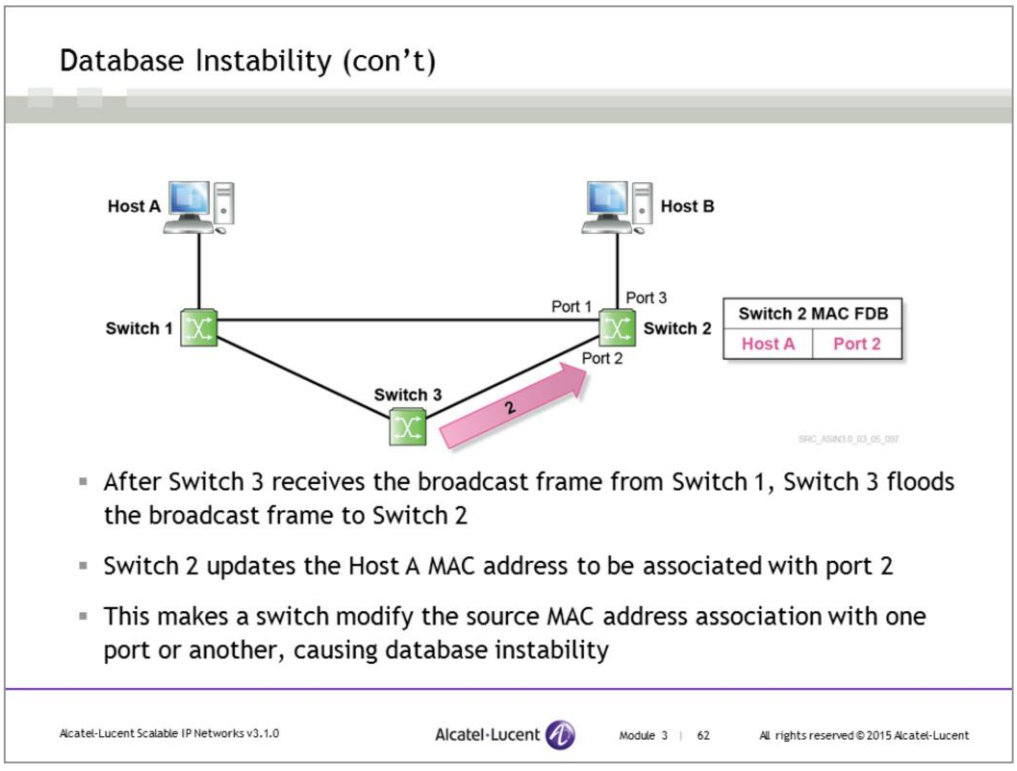


Redundant networks without STP can also cause database instability.

In this slide, Switch 2 first maps the MAC address of Host A to port 1.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

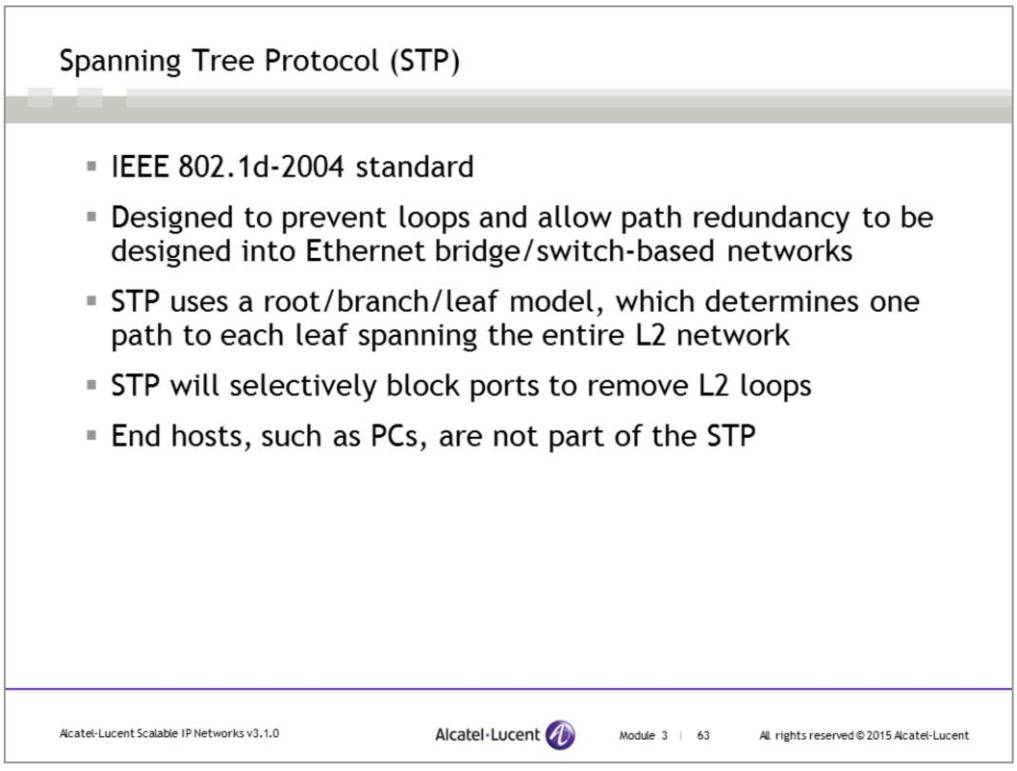


Later, when the copy of the frame arrives at port 2, Switch 2 must remove its original entry for Host A and replace it with the new entry for Host A, mapping it to Port 2. This activity causes an unstable database as Switch 2 tries to keep up with the perceived location of Host A.

When there are active redundant paths in an Ethernet switch network, frames can be forwarded indefinitely because of the way switches learn MAC addresses and flood frames with an unknown destination. What is needed is a way to preserve redundant paths while avoiding this problem.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



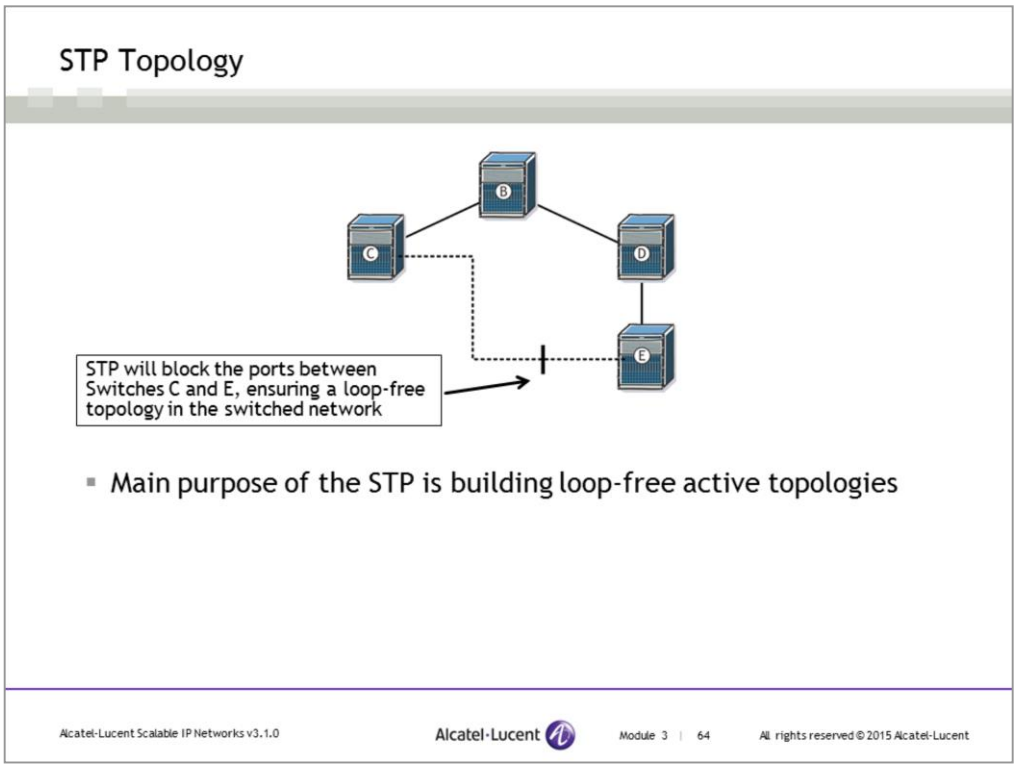
Spanning Tree Protocol (STP) was developed to solve the instability and broadcast storm issues.

STP is intended to prevent loops in an Ethernet network by selectively blocking ports to achieve a loop-free topology. STP determines what ports it can put into a non-functioning state to prevent loops from occurring, while still allowing frames to reach every destination in the Ethernet network. STP uses a root/branch/leaf model, which determines a single path to each leaf spanning the entire switched network. End stations, such as PCs, are not part of the STP protocol.

Note that STP is not a forwarding protocol, so an active path may not always be the optimal path.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The sole purpose of STP is to build an active loop-free topology. Blocked active ports can change in response to changed network conditions.

Spanning Tree topology can be thought of as a tree that includes the following components :

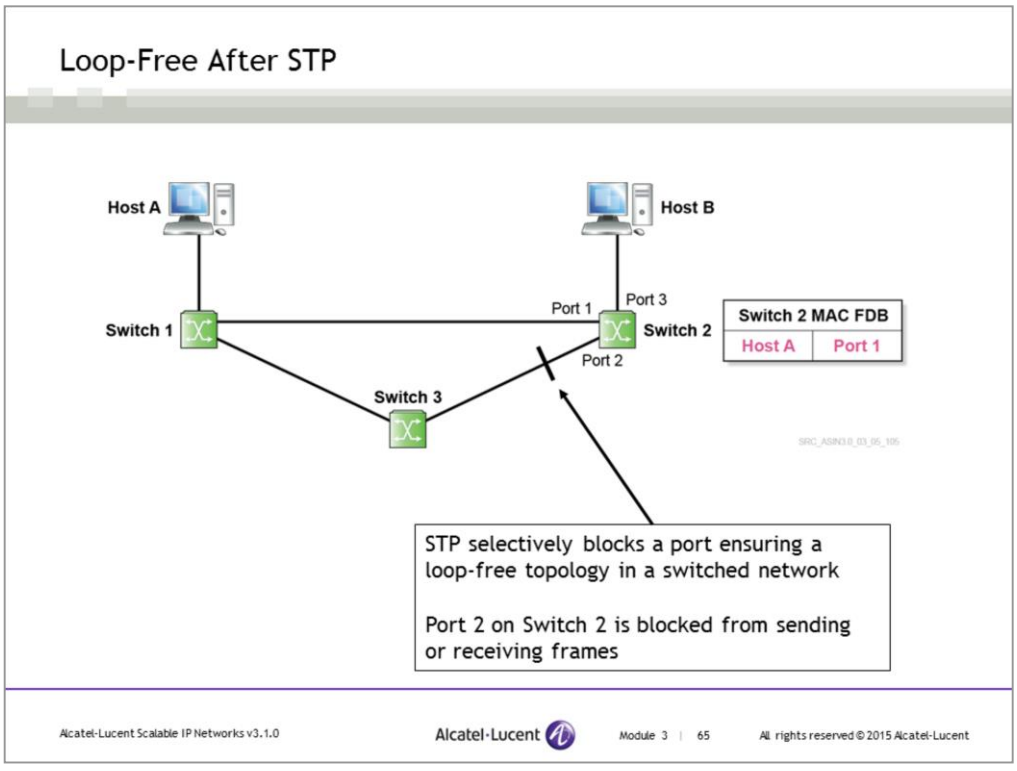
- a root (a root bridge/switch)
- branches (LANs and designated bridges/switches)
- leaves (end nodes)

There are no disconnected parts of the tree. That is, the tree encompasses all of its leaves. There are no loops in the tree. If you trace a path from one leaf to any other leaf, there is only one possible path. STP organizes and connects switches into a loop-free topology, while leaving no segments isolated.

More information about STP, refer to SRC VPLS course.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



There is still a redundant path in the Ethernet switched network. However, STP selectively sets one of the ports in the switched network to a blocking state. This port is blocked from sending or receiving frames, resulting in A loop-free switched network.

Consider the case where traffic has been transmitted on the above network. Therefore, both Switch 1 and Switch 2 have an empty MAC FDB:

1. Host A sends a broadcast frame. Switch 1 floods the broadcast frame to all ports except the receiving port.
2. Switch 2 receives the broadcast frame from Switch 1 on port 1.
3. Switch 3 also receives the broadcast frame from Switch 1. Since the port connecting to Switch 2 is blocked, the switch WILL NOT replicate the frame and sends it out of the port connected to Switch 2.
4. Switch 2 WILL NOT receive the replicated frame from Switch 3 because the port connecting to Switch 3 is blocked.
5. With a loop-free switched network, there will be no broadcast storm or MAC FDB instability.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

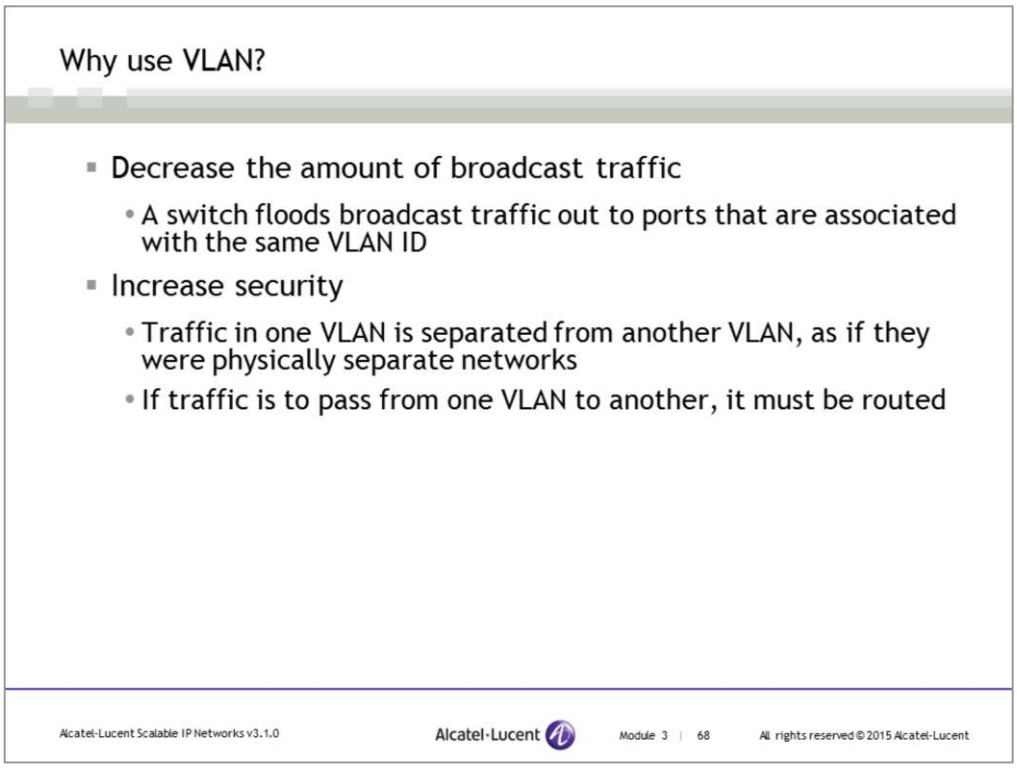
After successful completion of this section, you will be able to:

- Describe the benefits of VLANs
- Describe the use of VLANs in an Ethernet switch
- Describe the use of VLANs between switches and VLAN tagging
- List the Ethernet header fields used for VLAN tagging
- Describe the purpose of VLAN stacking

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 3 | 67
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



There are two main reasons for the development of VLANs:

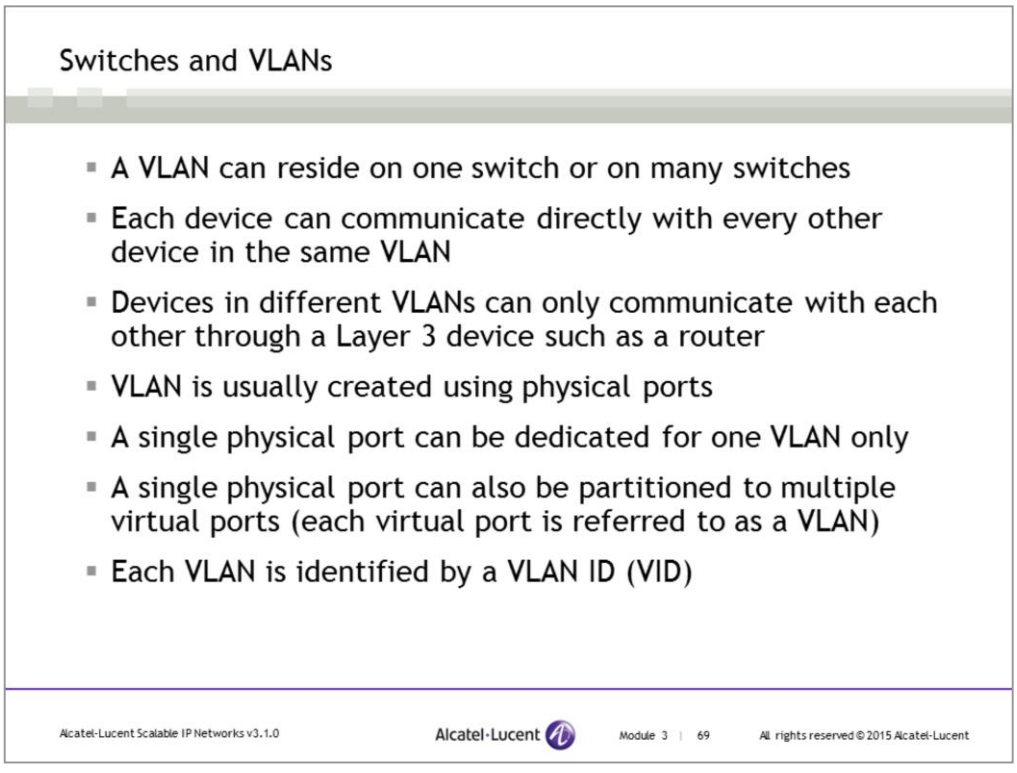
- the amount of broadcast traffic
- increased security

Broadcast traffic increases in direct proportion to the number of stations in the LAN. The goal of the virtual LAN (VLAN) is the isolation of groups of users so that one group is not interrupted by the broadcast traffic of another. By segregating a group of devices to a particular VLAN, a switch will block broadcasts from devices in that VLAN to devices that are not in that VLAN instead of flooding it out every port.

VLANs also have the benefit of added security by separating the network into distinct logical networks. Traffic in one VLAN is separated from another VLAN as if they were physically separate networks. If traffic is to pass from one VLAN to another, it must be routed.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

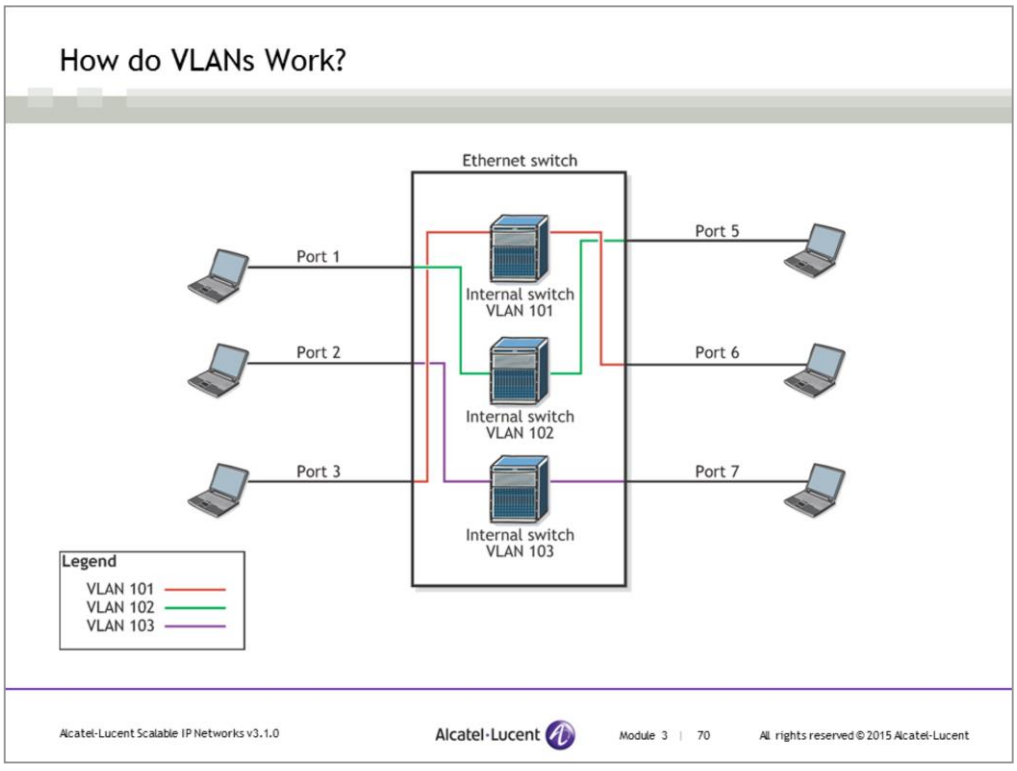


Each VLAN is identified by a VLAN ID (VID), which is usually a number. They can reside on only a single switch, or they can be distributed throughout the entire network on each switch. Each VLAN is a broadcast domain. Each device in a VLAN, regardless of its physical location, can communicate directly with every other device in the same VLAN. However, they cannot communicate outside of the VLAN except through a router. A VLAN is usually created using physical ports.

A single physical port can be dedicated for one VLAN only. A single physical port can also be partitioned to multiple virtual ports, where each virtual port is referred to as a VLAN. Even though a physical port can carry different customers' traffic on a single physical cable, each customer's traffic is completely isolated by using VLANs.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

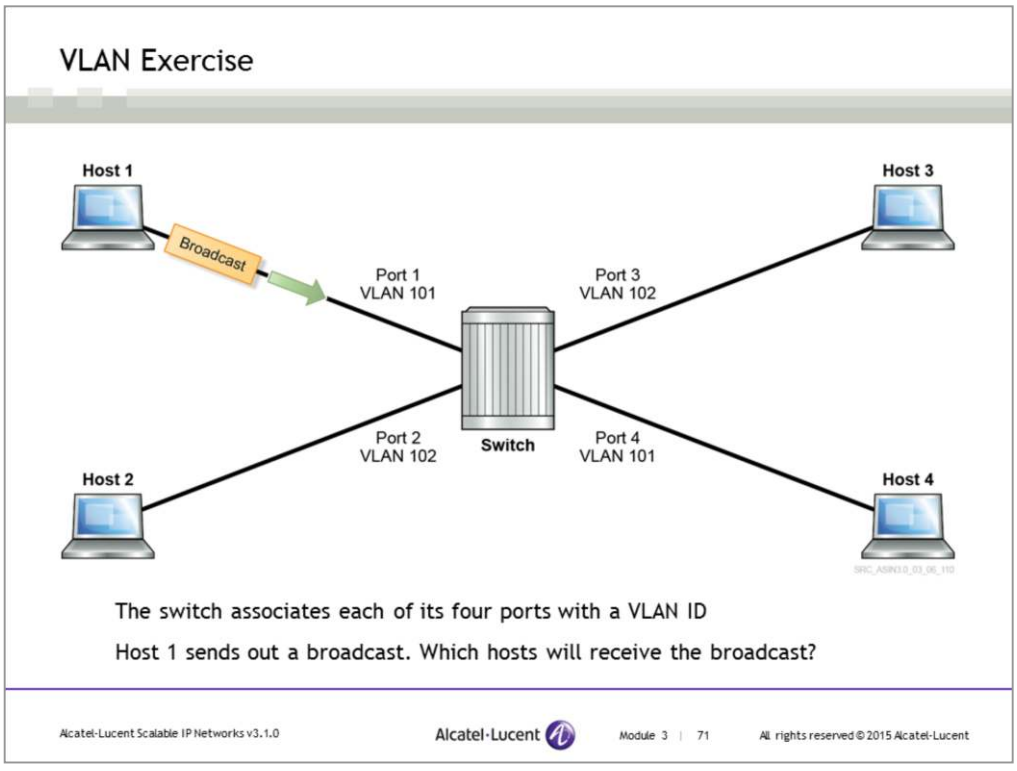


In this slide, VLANs subdivide the Ethernet switch into multiple switches. Note that there are no logical interconnections between these internal switches. Therefore, the broadcast traffic generated by a host in a VLAN stays within that VLAN, making the VLAN its own broadcast domain. Because broadcast traffic for a particular VLAN remains within that VLAN's borders, inter-VLAN or broadcast domain communication must occur through a Layer 3 device, such as a router.

Usually, hosts are not VLAN-aware, and therefore no VLAN configuration is required on the hosts. The VLAN configuration is done when the switch and ports are assigned on a VLAN-by-VLAN basis.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

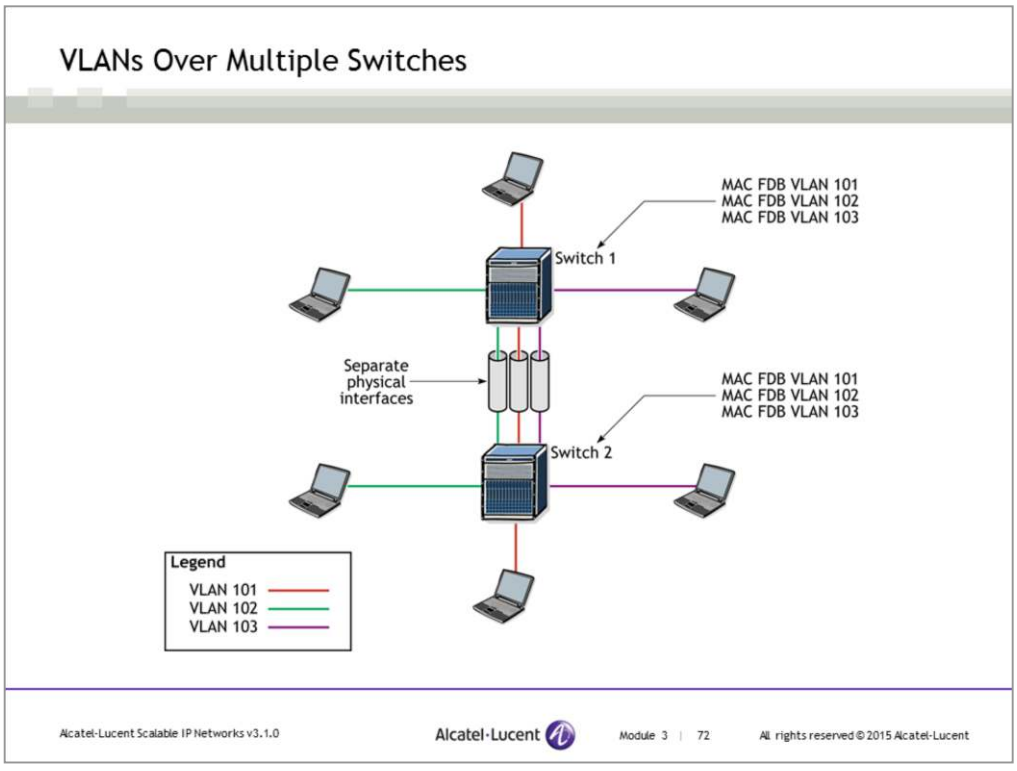


In this slide, Host 1 sends out a broadcast. Because Host 4 is the only other member of the VLAN, it is the only host to receive the broadcast.

The FDB entries behave much the same way in the VLAN model as they do in the standard switch model. They are updated based on the source address received on a given port. In this slide, the source address of the broadcast frame is only learned by VLAN 101 on the ingress port. VLAN 102 will not know the source address of Host 1 after Host 1 transmits its broadcast packet. Therefore, in a VLAN environment, a separate FDB is kept for each VLAN. In this case, this means that the FDB for VLAN 101 will never learn about Host 3 or Host 2 and the FDB for VLAN 102 will never learn about Host 1 or Host 4.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



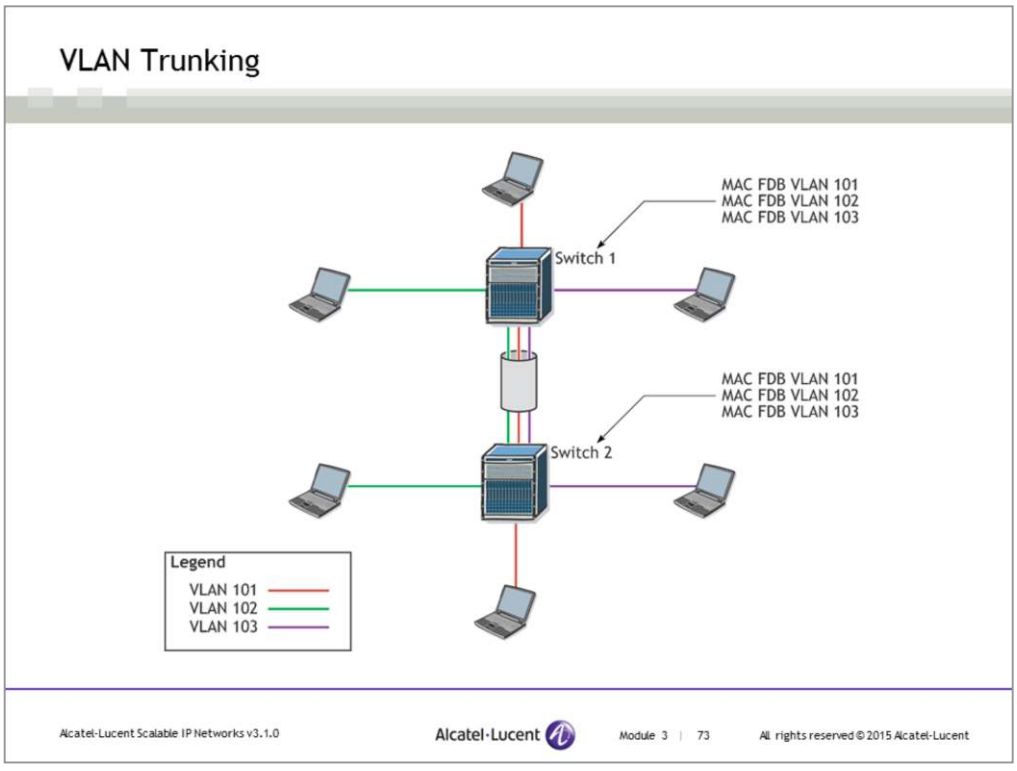
This slide indicates that three VLANs are shared across multiple switches. Frames ingressing a port in a particular VLAN will only be allowed to egress a port on the same VLAN. The VLAN can span across multiple switches because common VLAN information is configured on both Switch 1 and Switch 2. There are three physical links between Switch 1 and Switch 2, one for each VLAN.

The problem with this configuration is that it requires a separate physical link between the switches for each VLAN. Therefore, this configuration is not a very scalable or practical solution.

This slide indicates which ports belong to which VLAN. The traffic ingressing a port in one VLAN will only be allowed to egress a port on the same switch belonging to the same VLAN.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



VLAN trunking provides efficient interswitch forwarding of VLAN frames. In the previous slide, each VLAN required a separate interswitch connection to forward frames from one switch to another.

VLAN trunking allows one Ethernet port to carry frames from multiple VLANs. This allows the use of a single high-bandwidth port, such as a gigabit Ethernet port, to carry the VLAN traffic between switches instead of one port per VLAN.

VLANs are separated within the trunk based on their VLAN IDs (802.1Q tags). The FDB at the destination switch designates the destination VLAN for the traffic on the VLAN trunk.

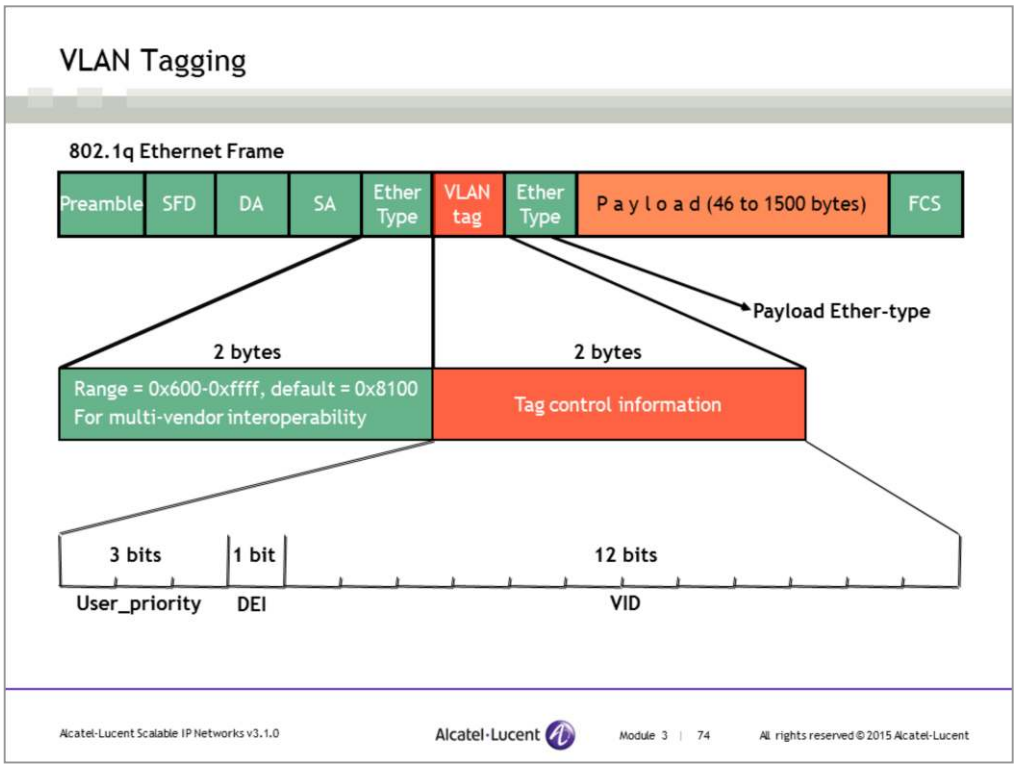
The sharing of VLANs between switches is achieved by the insertion of a header with a 12-bit VID, which allows for 2^{12} = 4094 possible VLAN destinations for each Ethernet frame. A VID must be assigned for each VLAN. Assigning the same VID to VLANs on different connected switches can extend the VLAN (broadcast domain) across a network.

When a frame leaves from a switch to another switch as its destination, the egress switch will tag the frames with a VID so that the ingress switch knows which VLAN the frame belongs to. The IEEE 802.1q standard governs the format of the assigned tag. The procedure works by inserting a 32-bit VLAN header into the Ethernet frame of all network traffic of the VLAN as it exits the egress switch. The VID uses 12 bits of the 32-bit VLAN header. The ingress switch then uses the VID to determine which FDB it will use to find the destination.

After a frame reaches the destination switch port and before the frame is forwarded to the end destination, the VLAN header is removed.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The VLAN header can be broken down into two parts: the VLAN tag type and the tag control information.

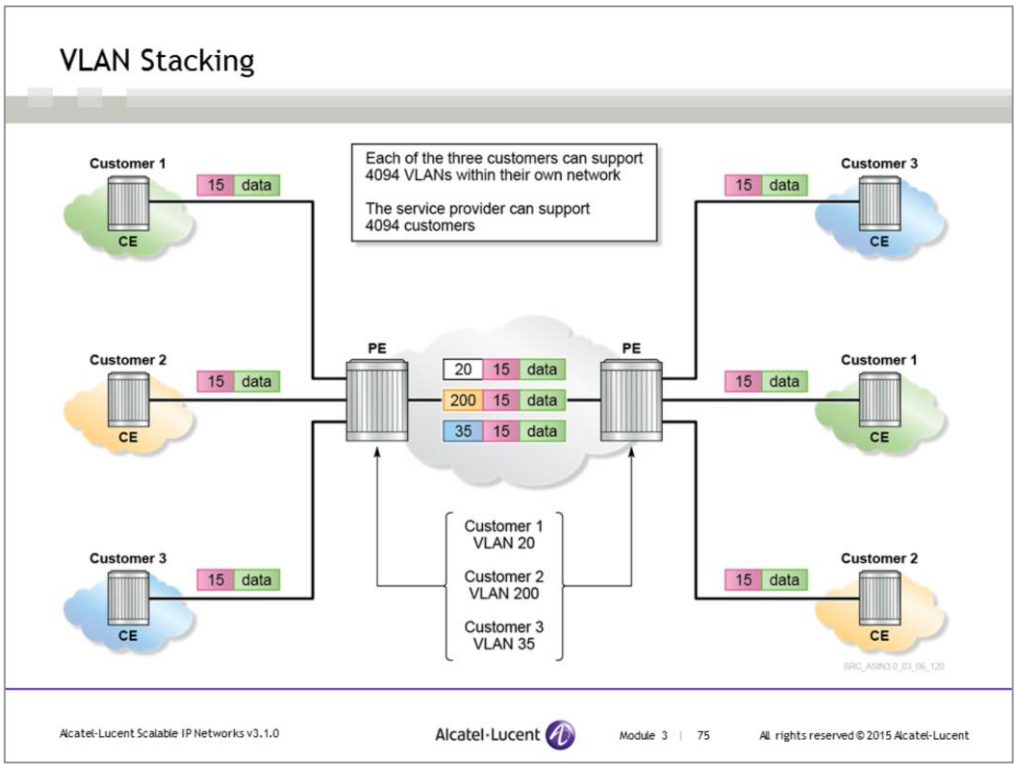
The VLAN tag type is a fixed-value indicator of a VLAN tag. The VLAN tag is a fixed length of 2 bytes, which is followed by the original Ethertype describing the payload.

The tag control information has three parts:

- **Priority value (User priority)** — A 3-bit value that specifies a frame's priority. There are eight user priority levels that provide information to network devices about the class of service that the frame should receive.
- **DEI (Drop Eligible Indicator)** — A 1-bit field that may be used separately or in conjunction with User Priority to indicate frames eligible to be dropped in the presence of congestion. When the DEI is set to 1, the frame is eligible to be discarded. DEI was formerly called Canonical Format Indicator (CFI).
- **VID** — A 12-bit value that identifies the VLAN that the frame belongs to. If the VID is 0, the tag header contains only priority information.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A restriction of Ethernet VLANs is the limited number of VIDs. With 12 bits used to define the VID, there are only 2^{12} = 4096 possibilities. Because VLAN 0 and 4095 are reserved, the Provider Edge (PE) router is really only capable of supporting 4094 VLANs — not a significant number if it is compared with the expanding rates of networks.

One of the solutions to this restriction is VLAN stacking, also known as Q-in-Q. VLAN stacking allows the service provider to use Layer 2 protocols to connect customer sites.

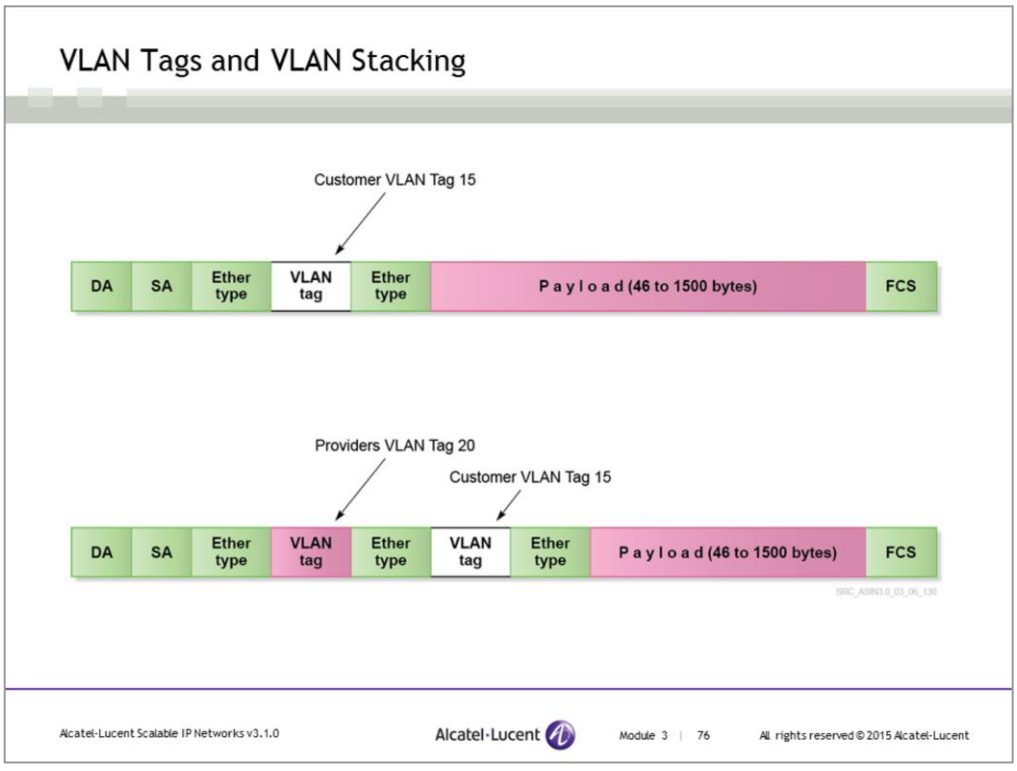
In this slide, three customers are connected through a common switch using VLAN stacking. Service providers can "stack" VLAN ID information to support multiple customers with overlapping VLANs over the same provider backbone.

At the PE, the administrator has assigned a VLAN to represent the customer on that port. When customer traffic arrives at the PE device, the PE switch inserts another VLAN tag in the frame in front of the first VLAN tag. It is this second or stacked VLAN tag that takes the customer traffic through the provider network. At the egress port of the PE equipment, the second or stacked VLAN tag is removed and the traffic forwarded out of the port.

This allows Customers 1, 2 and 3 to use the same VLAN tags in their network. In theory, the service provider can support 4094 customers, with each customer supporting 4094 VLANs within their network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In the example on the previous slide, Customer 1 sent a frame to the PE switch with a VLAN tag of 15. The PE switch inserts a second VLAN tag of 20. This tag number represents Customer 1 traffic. The second tag keeps Customer 1 traffic separate from Customer 2's and 3's traffic and gives Customer 1 the ability to add 4095 more associated VLANs.

The VLAN tag inserted by the provider is the VLAN tag that is used in the provider network. When the frame has reached the appropriate egress port, the provider's VLAN tag is removed and the frame with the customer's VLAN tag is forwarded out of the egress port.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Summary

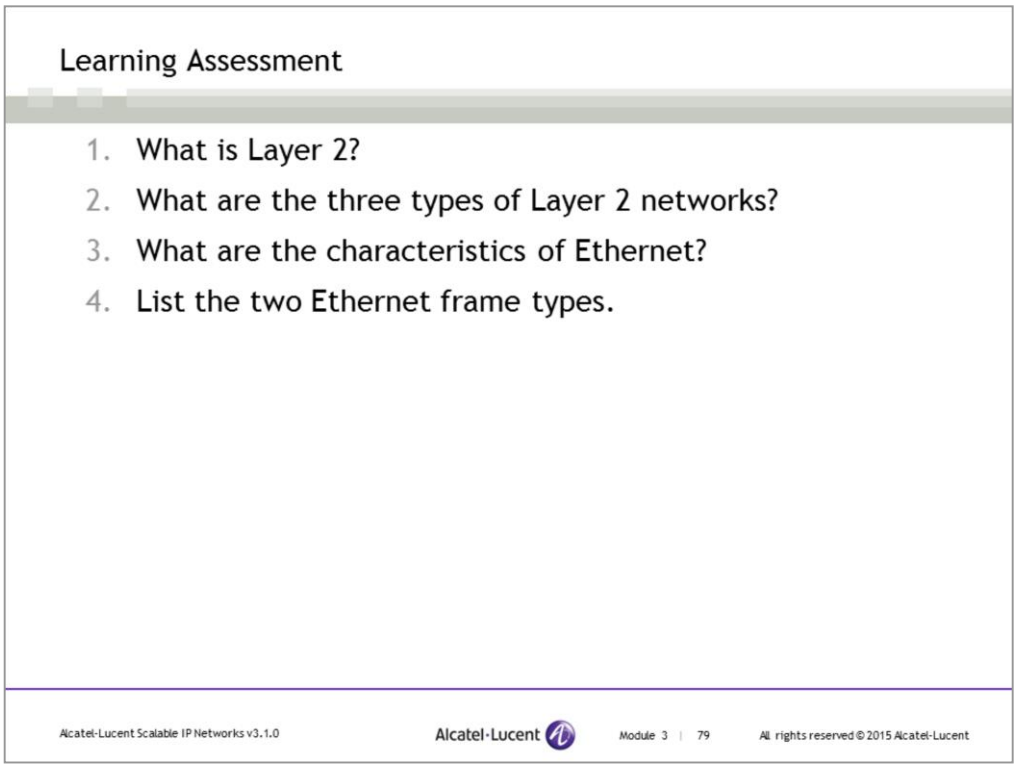
After successful completion of this module, you should be able to:

- Describe the characteristics of Layer 2
- Describe the characteristics of Ethernet
- Identify different types of Ethernet physical cabling
- Describe the purpose of a switch FDB and how it is populated
- Describe how a switch forwards unicast, multicast, and broadcast frames
- Describe different types of redundancy in an Ethernet-switched network
- Describe how virtual LANs can be used in one or more Ethernet switches

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

1. What is Layer 2?

Required as an interface between the underlying physical infrastructure and the upper layer; hides the details of the interaction with the physical medium entirely from the upper protocols so that the upper protocols do not need to have knowledge of the underlying physical infrastructure.

2. What are the three types of Layer 2 networks?

L2 protocols can be classified broadly into three types:

1) Point-to-Point Network: does not require source and destination addresses since they are established between two networking devices only.
2) Circuit-Based Network: creates virtual circuits between different devices over a shared infrastructure.
3) Shared Network: provides each device with a share of underlying network medium, such as a physical cable or a switch.

3. What are the characteristics of Ethernet?

Ethernet is a broadcast technology that relies on a shared media for communication.

It uses a “passive” wait-and-listen protocol called CSMA/CD to handle frame collision on a shared media.
It uses MAC addresses to send data frames to all devices on the network.

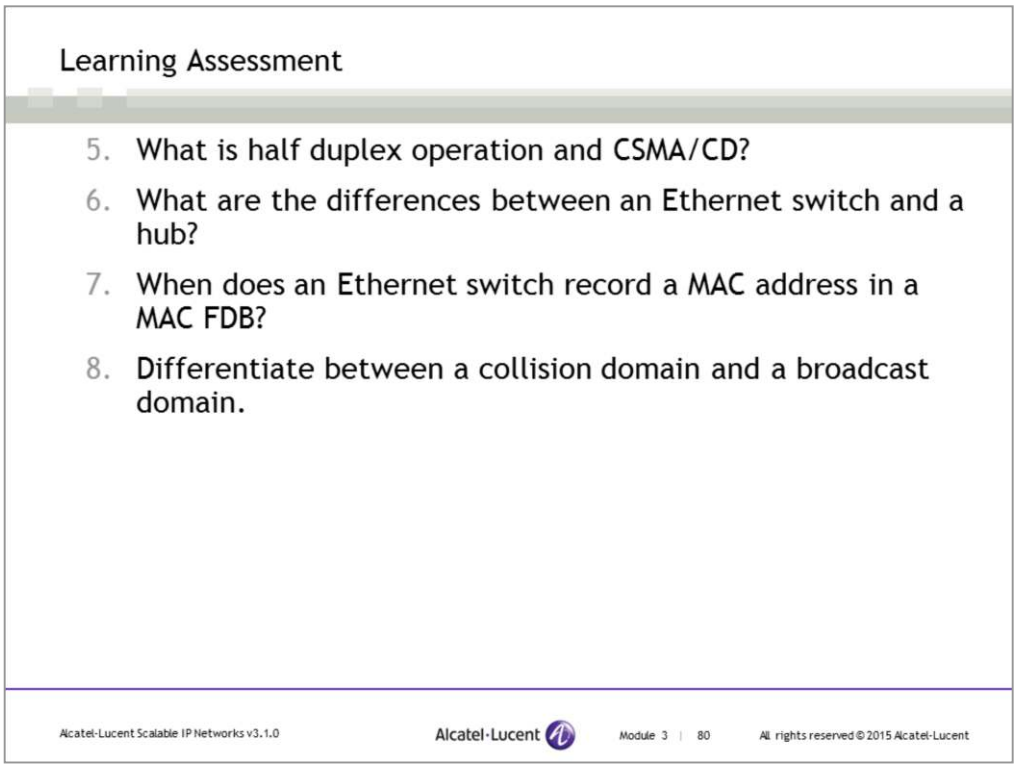
4. List the two Ethernet frame types.

Ethernet II and 802.3

The 16-bit field that follows the source address (SA) indicates whether the frame is Ethernet II or 802.3. If the EtherType or length value is less than 1536, the frame is treated as 802.3. If the value is 1536 or greater, the frame is treated as Ethernet II. An Ethernet II frame is normally used for transmission of IP datagrams.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

5. What is half-duplex operation and CSMA/CD?

All hosts constantly listen to the shared media. When a host transmits, all other hosts listen to the sending host and do not transmit. All hosts receive frames from the sending host.

CSMA/CD is a protocol used reduce the chance of collision and handle those that occur, but it does not and cannot prevent them. When two hosts transmit frames at the same time, they will both detect collision. Both hosts will generate a jam signal to notify all other hosts. A random back-off timer is then started on the two transmitting hosts. Afterward, either of the hosts will initiate a transmission after they detect no other transmission on the line.

6. What are the differences between an Ethernet switch and an Ethernet hub?

An Ethernet switch provides full-duplex capabilities and avoids collision. An Ethernet switch can make an intelligent forwarding decision and send frames only to the port that needs to receive them.

The hub, on the other hand, provides half-duplex capabilities and collisions can occur. Any Ethernet frame that arrives on a port is automatically forwarded out to all other ports.

7. When does an Ethernet switch record a MAC address in a MAC FDB?

When an Ethernet switch receives an Ethernet frame, it records the source MAC address and the interface on which it arrived into a MAC forwarding table (FDB).

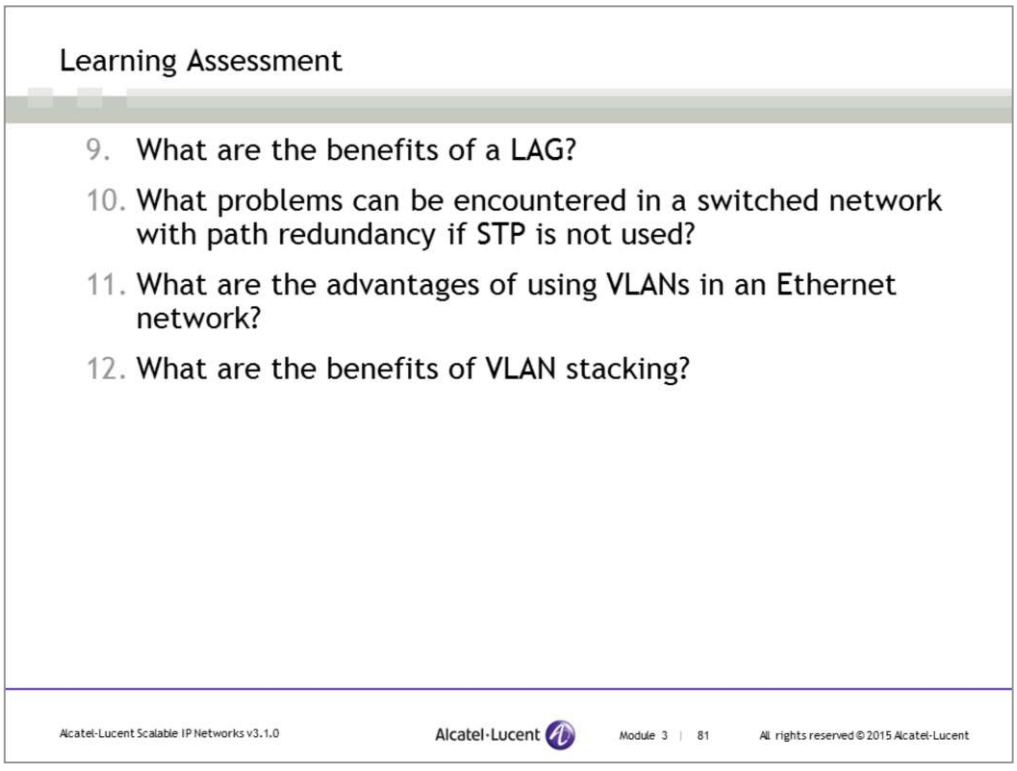
8. Differentiate between a collision domain and a broadcast domain.

In a collision domain, only one Ethernet device can transmit at any one time, and the other devices in the domain listen to the network to avoid data collisions.

In a broadcast domain, every Ethernet device will receive and process all broadcast packets.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

9. What are the benefits of LAG?

LAG is used to provide link redundancy. LAG aggregates multiple physical links between Ethernet devices so that they are functionally equivalent to a single logical link.

The primary benefits of LAG are:

1) Increases the bandwidth available between two Ethernet devices by grouping multiple ports into one logical link

2) Provides link redundancy between devices

10. What problems can be encountered in a switched network with path redundancy if STP is not used?

1) Broadcast storm due to constant "looping" of Ethernet frames

2) FDB table instability as switches might see a frame with a source address that comes from a different interface than the existing entry in the MAC FDB

11. What are the advantages of using VLANs in an Ethernet network?

1) To decrease the amount of broadcast traffic – broadcast traffic from a device within a VLAN is only received by other devices within the same VLAN. Devices in a different VLAN do not receive that broadcast traffic

2) To increase the network security – traffic in one VLAN is separated from another VLAN as if they are physical separate networks

12. What are the benefits of VLAN stacking?

1) Solves the problem caused by Provider Edge (PE) routers only supporting 4,094 VLANs

2) Allows multiple customers with the same VLAN tag in their network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Objectives

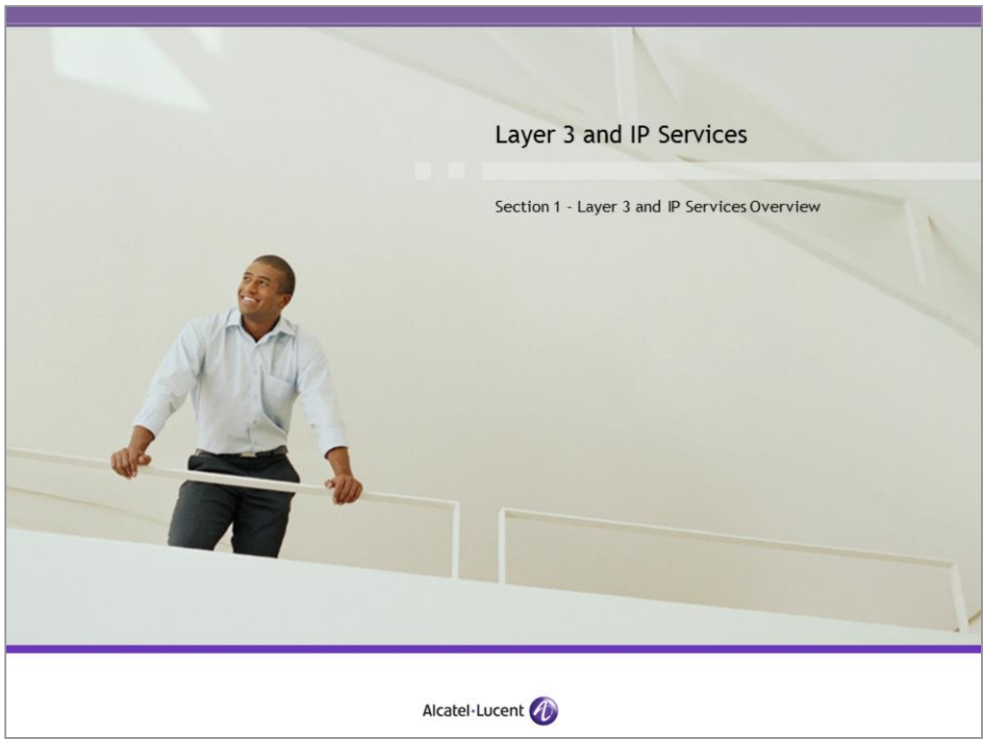
After successful completion of this module, you will be able to:

- Describe the function of Layer 3
- Describe the basics of IP addressing
- Describe the purpose, components, and operation of the IP subnet address
- Develop an IP address plan using IP subnetting and addressing summarization
- Describe the IP address forwarding process
- Describe other protocols that support IP operation

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

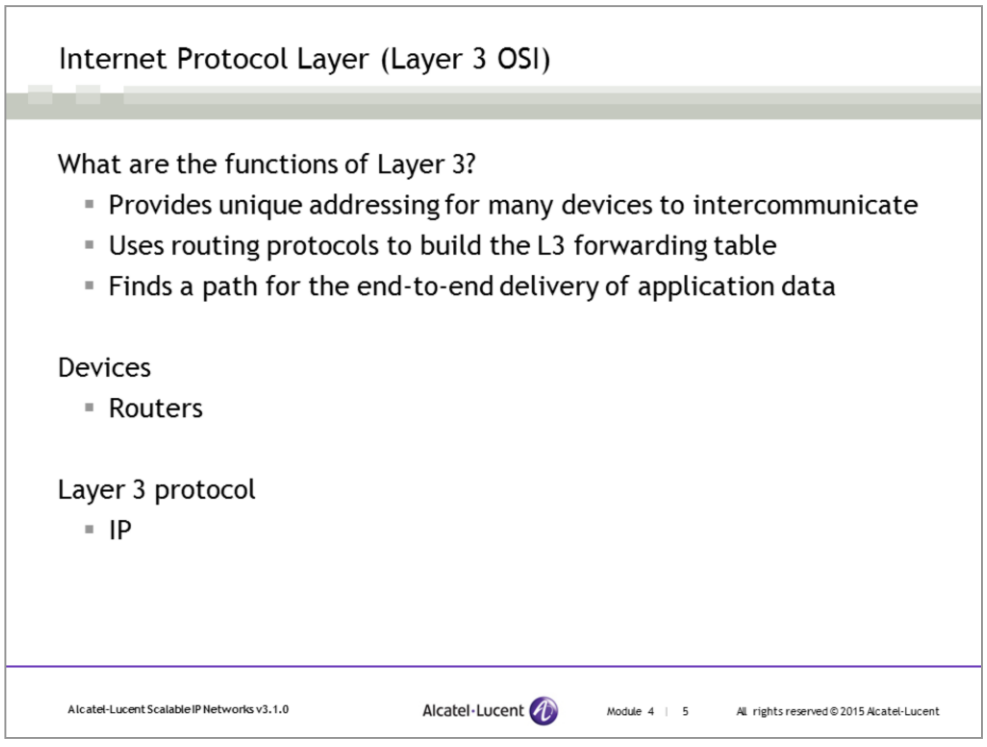
After successful completion of this section, you will be able to:

- Describe the basic characteristics of IP
- Describe the requirement of using Layer 3 to connect multiple Layer 2 networks

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The network layer, or Layer 3 (L3), is considered the lowest layer in the TCP protocol stacks that handle the end-to-end delivery of application data. In this context, end-to-end means that IP is the first layer that can deliver information from any IP-capable device to any other IP-capable device, regardless of underlying Layer 2 technologies. The main function of L3 is to move data from the source to its destination, or set of destinations, regardless of where the destination is located. L3 performs this function by using a unique logical address and a standard set of protocols to help forward data based on the addressing scheme. Although a number of L3 protocols are still in use, Internet Protocol (IP) is almost exclusively used today.

From the source, the data must pass through various physical mediums across several Layer 2 domains over routers before reaching its destination(s). Routers inspect the IP header before forwarding data to the appropriate interfaces.

The IP address is a logical address that differs from a Layer 2 address. A layer 2 address, such as a MAC address, is permanently programmed into the firmware. The IP address uniquely identifies the device on the Internet. Address distribution is controlled by the Internet Assigned Number Authority (IANA), a global authority. The IANA ensures that every Internet address is unique. To ensure that data is sent to its correct destination, every device on the Internet must have a unique IP address.

Routing protocols are required to forward the data. Routers use the routing protocols to build forwarding tables. When an IP packet is received, the router checks the forwarding table to identify the physical interface destination for the data. Typically, several routers are involved in an end-to-end data transfer.

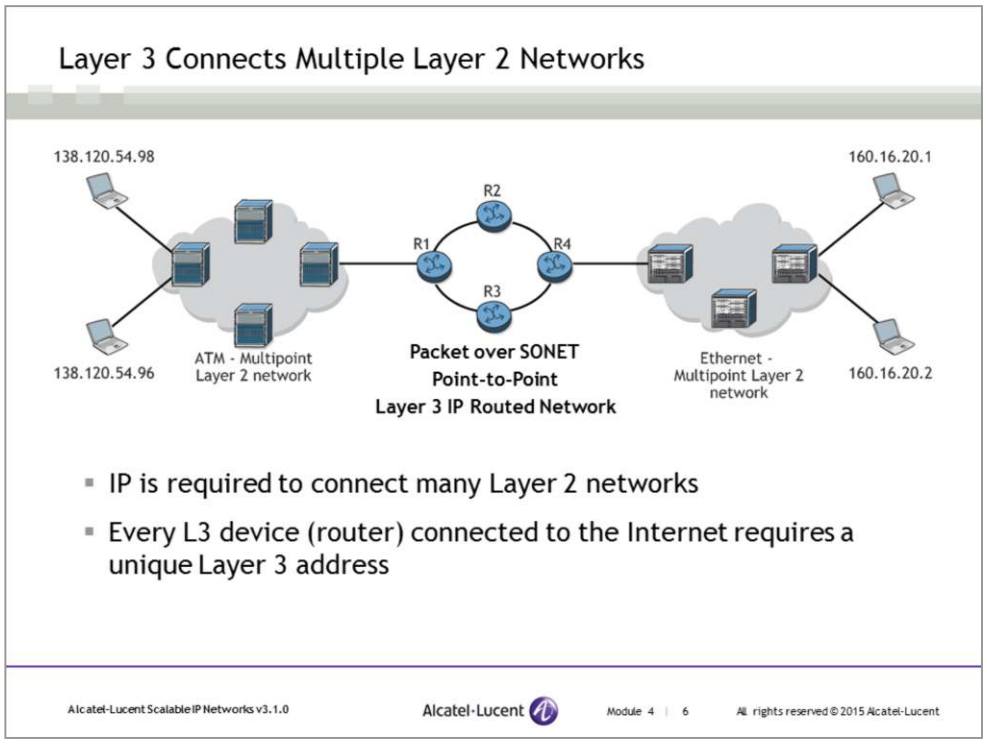
The most widely used L3 protocol is IP. IP provides a datagram (connection-less) transport service across the network. This service is referred to as ‘unreliable,’ because the network does not guarantee delivery or notify the end host system about packets lost because of errors or network congestion. Note that it does not mean that IP is unreliable and drops a large number of packets. It simply means that IP itself does not worry about packet loss, but instead relies on upper layer protocols, such as Transmission Control Protocol (TCP), to handle re-transmission in the event of dropped packets. In addition to providing unique addressing and data forwarding, L3 can make use of quality of service (QoS) to allow

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

different network traffic to be prioritized and forwarded differently by the intermediate routers.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



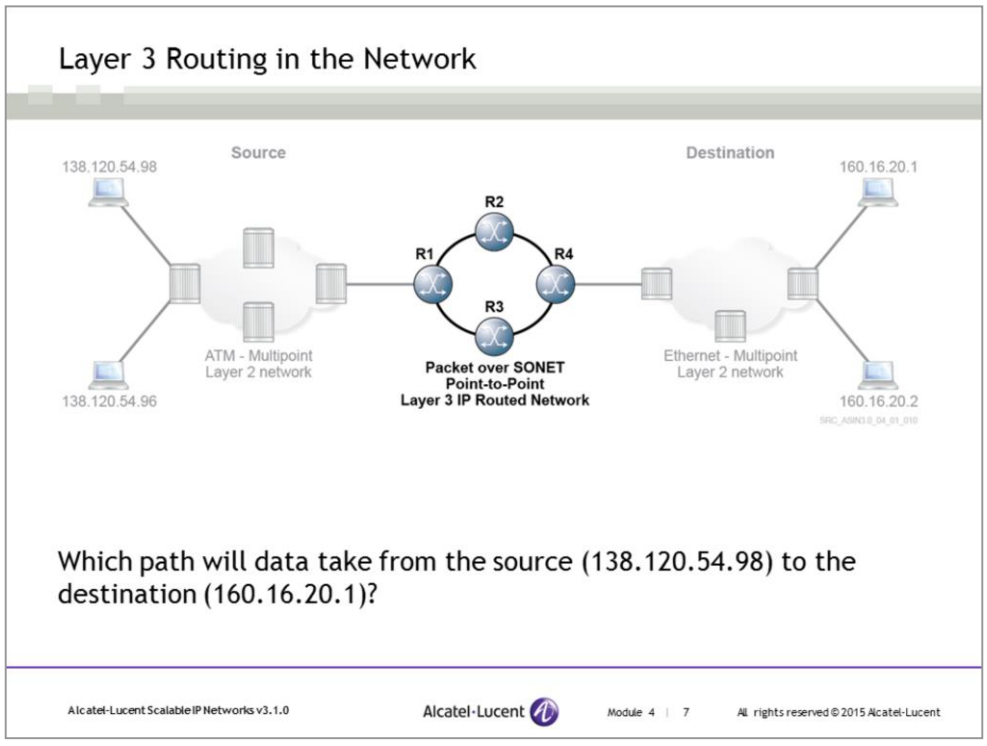
In this slide, end-hosts on ATM need to communicate with end-hosts on Ethernet over a POS network. This situation requires IP to transfer the information from one L2 network to another.

IP is required because the physical networks that are connected to the user PCs are different in each location. One of the networks is ATM, one is Packet over SONET (POS), and one is Ethernet. It would be very difficult, if not impossible, for a simple L2 switch to transmit a frame from one end-host to another in this scenario.

The IP layer is required to direct the data from the source PC to the destination PC. The routers (as will be seen later) are responsible for directing the data based on information in the IP header. The TDM, ATM, POS, and Ethernet-based switches transmit the IP datagrams between the routers. The routers inspect the IP header and direct the data to the appropriate interface based on its IP address in the forwarding table.

 All rights reserved © 2015 Alcatel-Lucent

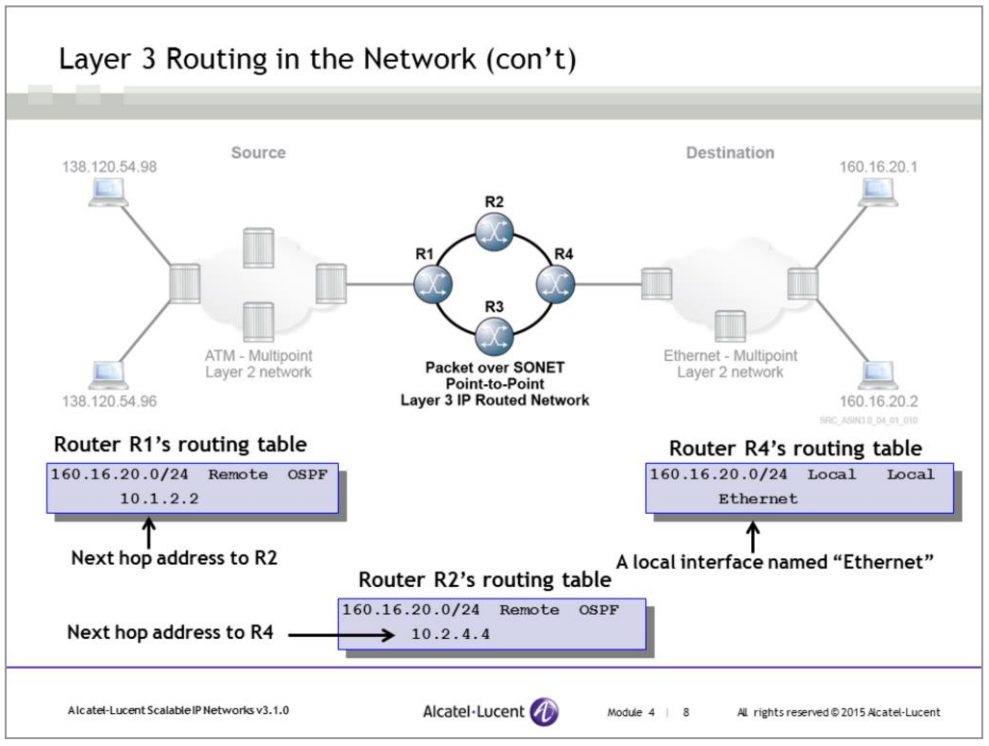
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, the IP address of the data source is 138.120.54.98/24 and the IP address of the destination is 160.16.20.1/24. Because the destination is not on the same Layer 2 network as the source, the data will travel to the router that is attached directly to the Layer 2 switch in the ATM network using Layer 2 forwarding. The router (R1) must then send the packet out of one of its directly connected interfaces to either router R2 or R3. R2 or R3 will, in turn, send the packet to its directly connected interface to router R4. R4 will send the data to its directly connected L2 switch on the Ethernet network. Since the destination is in the Ethernet network, the L2 switch will forward the data to the destination using Layer 2 forwarding.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Before router R1 can decide which interface it should send a packet with a destination address of 160.16.20.1, R1 needs the knowledge to do so. This knowledge is created using routing protocols that run on all routers to create the L3 forwarding table, also known as a routing table. Routing tables are constructed on every router using routing protocols. When a packet arrives at a router, that router will check its routing table to find out which outgoing interface the packet should be sent to.

Every router on the network builds a routing table using routing protocols such as OSPF. When data arrives at the router, it uses the routing table to determine the next hop to the destination. The routing table contains a list of network destinations with the next hop address or the next hop interface, which tells the router how to reach the destination.

In this slide, router R1 needs to send a packet with a destination IP address of 160.16.20.1. R1 will check its routing table to determine which next hop router it should send the packet to.

R1 finds a network address of 160.16.20.0/24 with a next hop address pointing to router R2. (Note that more details about the network address will be discussed later in this module). Therefore, R1 sends the packet to the next hop router, R2.

Similarly, R2 finds a matching network address of 160.16.20.0/24 with a next hop address pointing to router R4. Therefore, R2 sends the packet to the next hop router, R4.

Finally, R4 finds a network address of 160.16.20.0/24 with a next hop interface named "Ethernet". Therefore, R4 sends the packets out of its locally connected interface named "Ethernet".

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

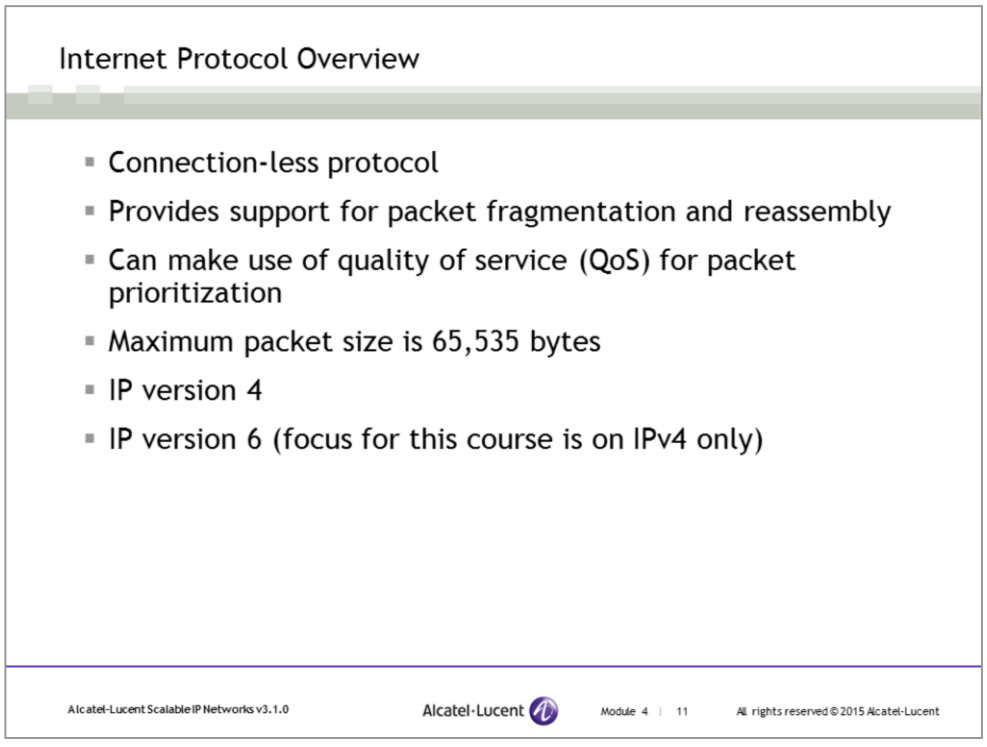
After successful completion of this section, you will be able to:

- List the entities responsible for address allocation
- List blocks of private IP address space
- List various fields in the IPv4 packet header
- Explain the purpose of each IP address type
- Explain the components of the dotted-decimal IPv4 address

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 4 | 10 All rights reserved © 2015 Alcatel-Lucent

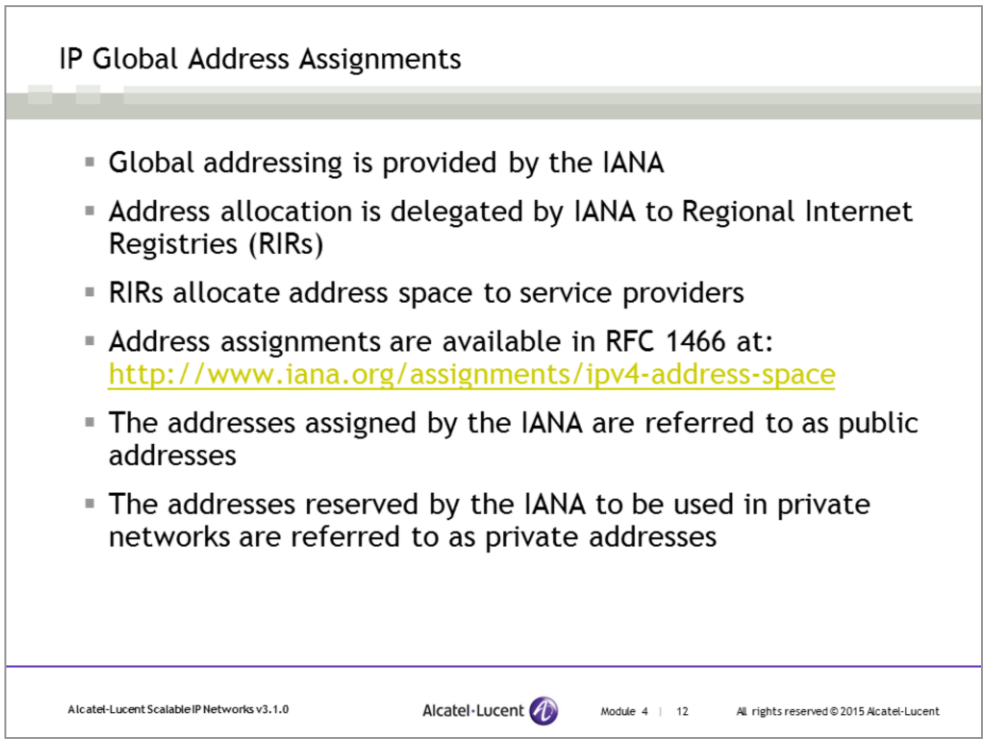
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Internet Protocol (RFC 791) provides services that are roughly equivalent to the OSI network layer. IP provides a datagram (connection-less) transport service across the network. This service is sometimes referred to as 'unreliable' because the network does not guarantee delivery or notify the end host system about packets lost due to errors or network congestion. IP relies on upper layer protocols, such as Transmission Control Protocol (TCP), to handle re-transmission in the event of dropped packets.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



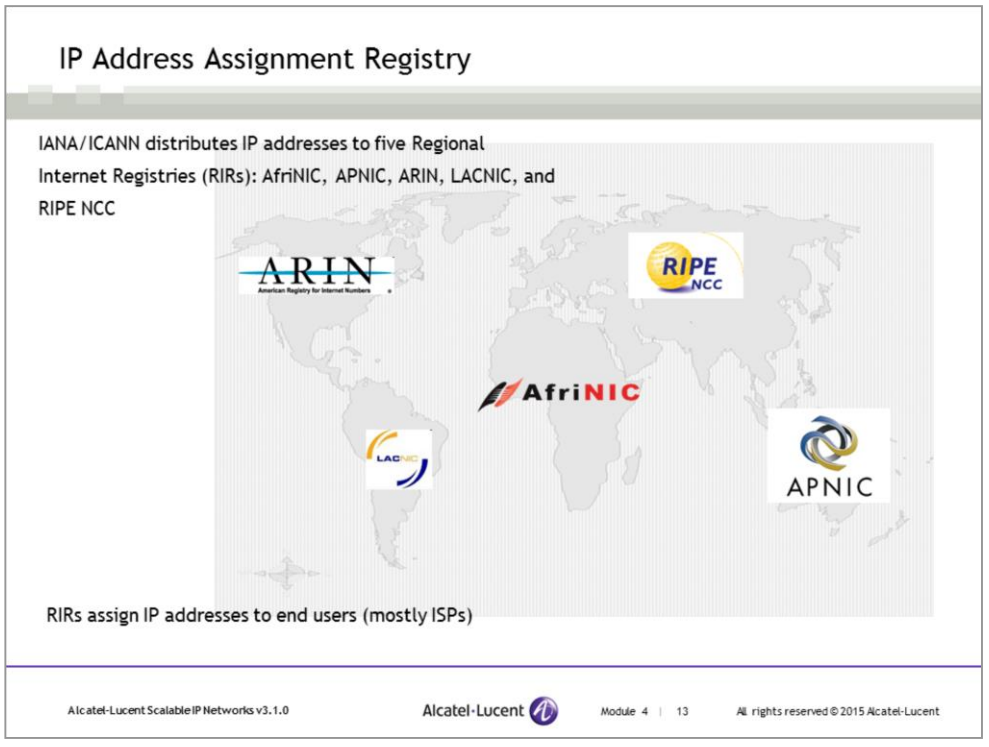
Under the current IP addressing scheme (known as IPv4, eventually to be replaced by IPv6), the address space is divided into two types: public address space and private address space. Understanding the difference is important and useful for a network administrator, especially if your organization is connected to the Internet. All IP addresses (public address space) that are routable by using the Internet are managed by a Regional Internet Registry (RIR). Each RIR is responsible for a geographic region.

Note: This should not be confused with the InterNIC (http://www.internic.net) and its designated registrars, such as Network Solutions, Inc. These organizations handle domain name registration, not address registration.

The IANA distributes IP addresses to the RIRs. Address space must be requested from IANA, which approves or denies each request. Alternatively, you can request the address space from your ISP. The ISP then allocates the space from its allotted address space or makes the request on your behalf. This system preserves address space and provides a central authority that prevents address-space collisions. When you use a public address, you can both send data to and receive data from all parts of the Internet. This means that all routers on the Internet can route your IP address to you.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



For the Internet to operate, the components need a common method of communication and common addressing for all physical components. Internet protocol (IP) provides a common method of communication and addressing.

Every device that connects to the Internet, or that communicates with another computer on the Internet, has a unique IP address. An example of an IP address is 138.120.105.45. This address must be unique to a single computer. Delivering packets to a given IP address is very similar to the methods of delivering mail to a person's home.

IP addresses are distributed and controlled by a centralized authority known as the Internet Assigned Numbers Authority (IANA). The IANA is operated by the Internet Corporation for Assigned Names and Numbers (ICANN).

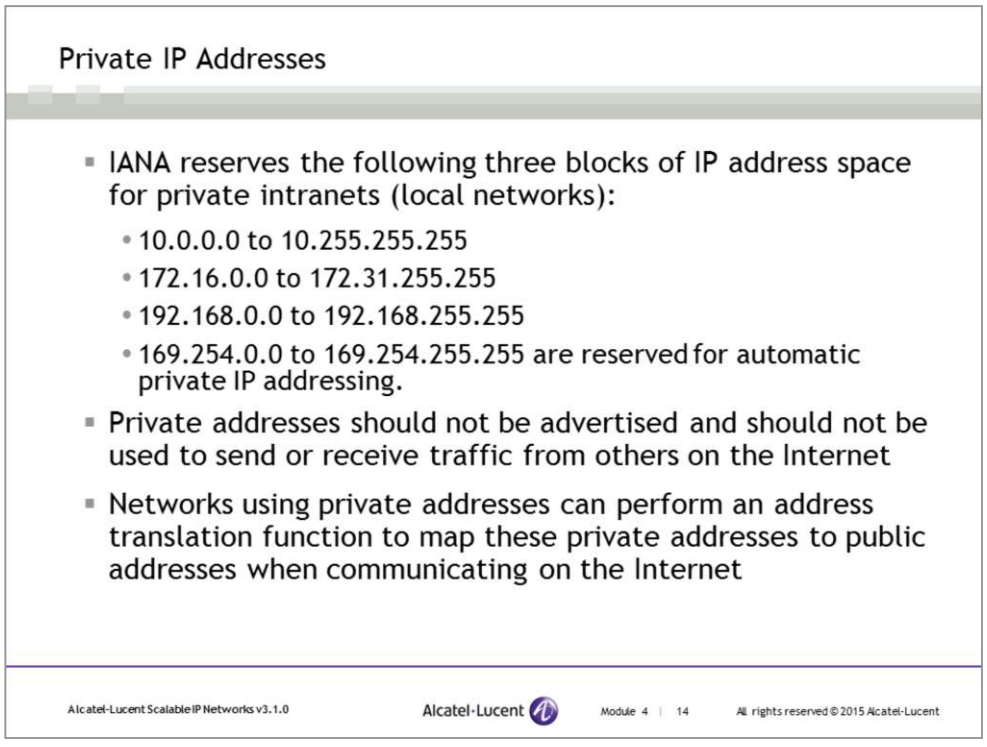
ICANN/IANA governs the global allocation of all possible address space used in the Internet to the 5 Regional Internet Registries. Each Regional Internet Registry (RIR) assigns chunks of address space to end users (mostly ISPs) based on their specific regional policies.

The five regional registries are:

- African Network Information Center (AfriNIC)
- Asia Pacific Network Information Centre (APNIC)
- American Registry for Internet Numbers (ARIN)
- Latin America and Caribbean Network Information Centre (LACNIC)
- Réseaux IP Européens Network Coordination Centre (RIPE NCC)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IANA has reserved the following three blocks of IP address space for private Internet (local networks):

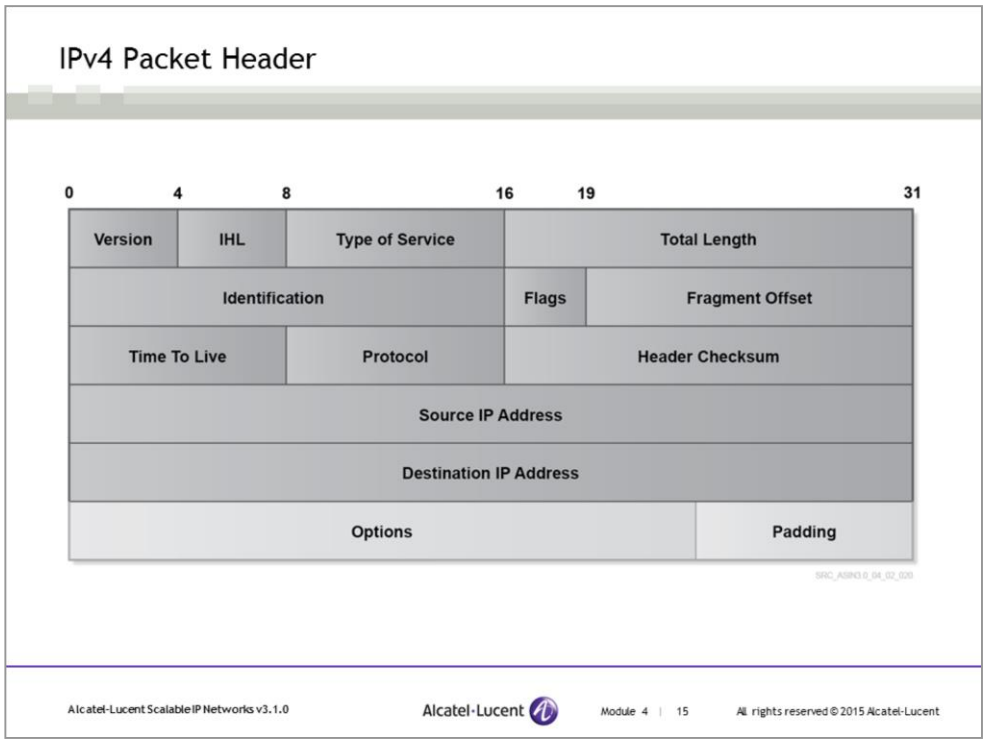
- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255
- IP addresses from 169.254.0.0 to 169.254.255.255 are reserved for automatic private IP addressing. These IP addresses should not be used on the Internet.

Any organization can use these private addresses in whatever way they want. They just cannot advertise them on the Internet or expect to send or receive traffic from other organizations using these addresses. These addresses are private and are expected to remain within a particular organization. It is quite common to find most customers using one or multiple of these address ranges in their internal network, performing an address translation function to map these addresses to public addresses for communicating to other devices on the Internet.

Private IP addresses should not be used on the Internet. If an inbound packet is sent to a local network with a source address in the private address range, there is either a configuration error on the sending device, or it was an attempt by an attacker to obfuscate the origin of the sending device. A packet with a destination address in this range cannot be forwarded, so any incoming packets from this source is essentially a dead end. The message cannot be returned.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Version — Always set to the value of 4, which represents IP version 4. There is also IP version 6, which uses a different IP header. Only IPv4 is discussed in this course.

IHL (IP Header Length) — A 4-bit field that contains the number of binary words (a word is 32 bits or 4 bytes) forming the header. This value is usually five.

TOS (Type of Service) — An 8-bit field that consists of a 6-bit Differentiated Services Code Point (DSCP) field and a 2-bit Explicit Congestion Notification (ECN) field. The TOS field defines the way routers should queue packets while they are waiting to be forwarded and, in some cases, allows packets to be forwarded along different paths based on priority.

Total Length — A 16-bit field specifying the total length of the packet, including the header, in bytes. The combined length of the header and the data can be at most 65,535 bytes. This is the largest possible decimal number that can be described by 16 bits in binary.

Identification — In conjunction with the source address, this 16-bit number uniquely identifies the packet. The number is used during the reassembly of fragmented datagrams. IP allows an intermediate router to break an IP packet into smaller pieces in case a large packet needs to be forwarded over a network that supports only smaller packets.

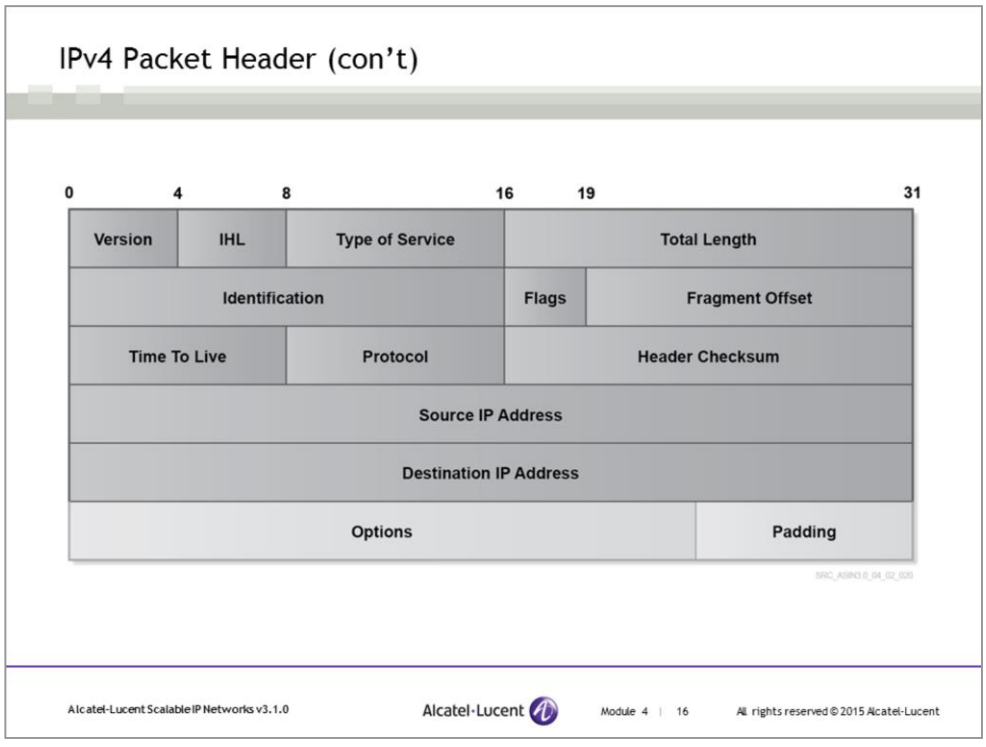
Flags — Three bits used to control whether routers are allowed to fragment a packet (Don't Fragment (DF) flag) and whether this packet is the last fragment (More Fragment (MF) flag).

Fragment Offset — An offset value from the start of the original packet, set by any router that performs IP fragmentation. It is not used if fragmentation is not performed.

(….continued on next slide)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



(….continued from previous slide)

Time To Live — Number of hops or links that the packet may be routed over, decremented by each router (used to prevent accidental routing loops). The TTL field ensures that all IP packets have a limited lifetime.

Protocol — A 8-bit identifier that indicates the type of transport packet being carried (for example, 1 = ICMP, 2= IGMP, 6 = TCP, 17 = UDP)

Header Checksum — This is a field for detecting errors in the IP header. The checksum is calculated by the transmitting router based on the contents of the IP header. It is calculated again by the receiver and compared with the value in the header. If they are different, the packet is discarded.

Source IP Address — A 32-bit IP address of the original sender of the packet

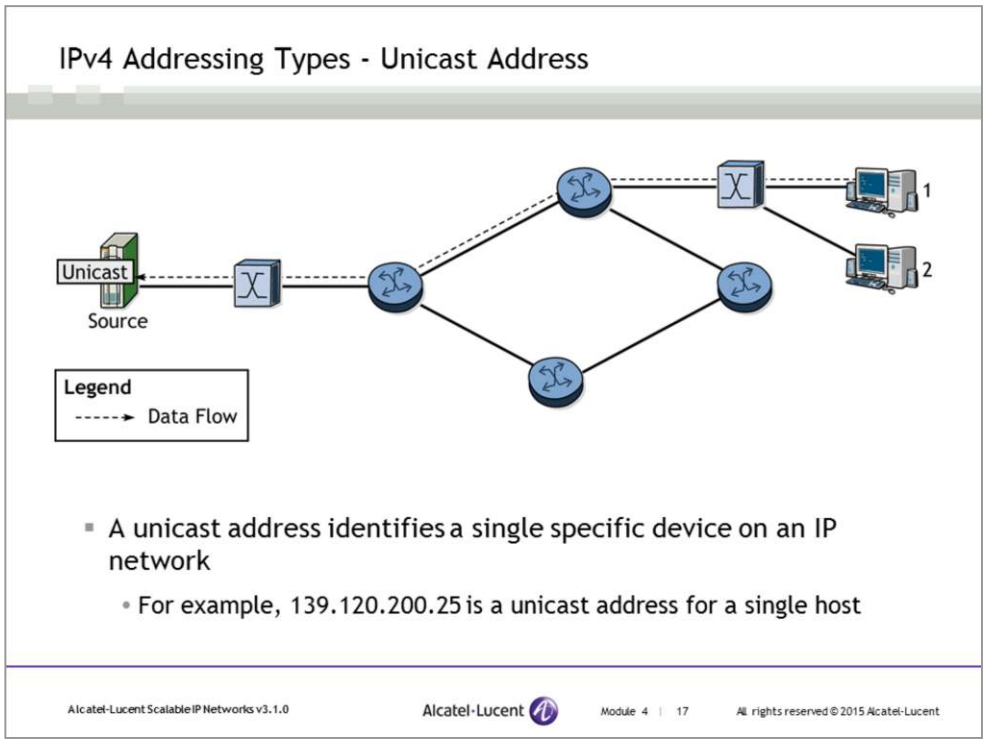
Destination IP Address — A 32-bit IP address of the final destination of the packet

Options — Not often used. However, when the options are used, the IP header length is greater than five 32-bit words to indicate the size of the options field.

Padding — Ensures the header ends on a 32-bit boundary in the event that options are used.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

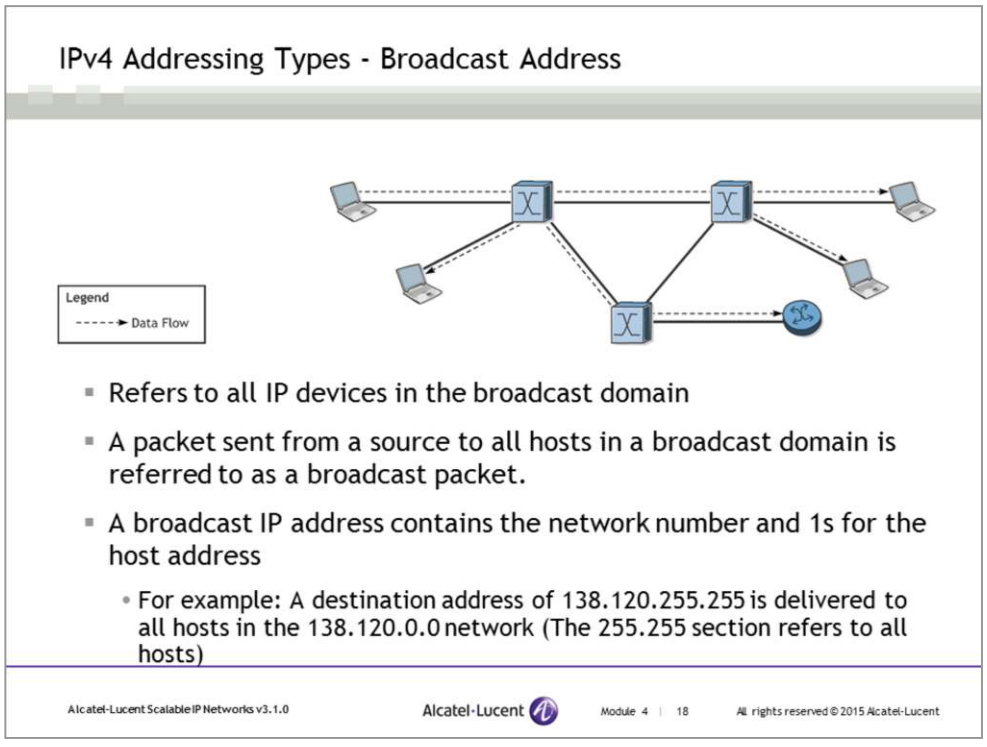


A unicast address refers to a specific IP address. A packet sent from a source to a specific destination address is referred to as a unicast packet. This packet is delivered to a single host or a single interface on the router.

This slide shows a unicast packet being delivered from a source to a single host, PC 1, across the network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

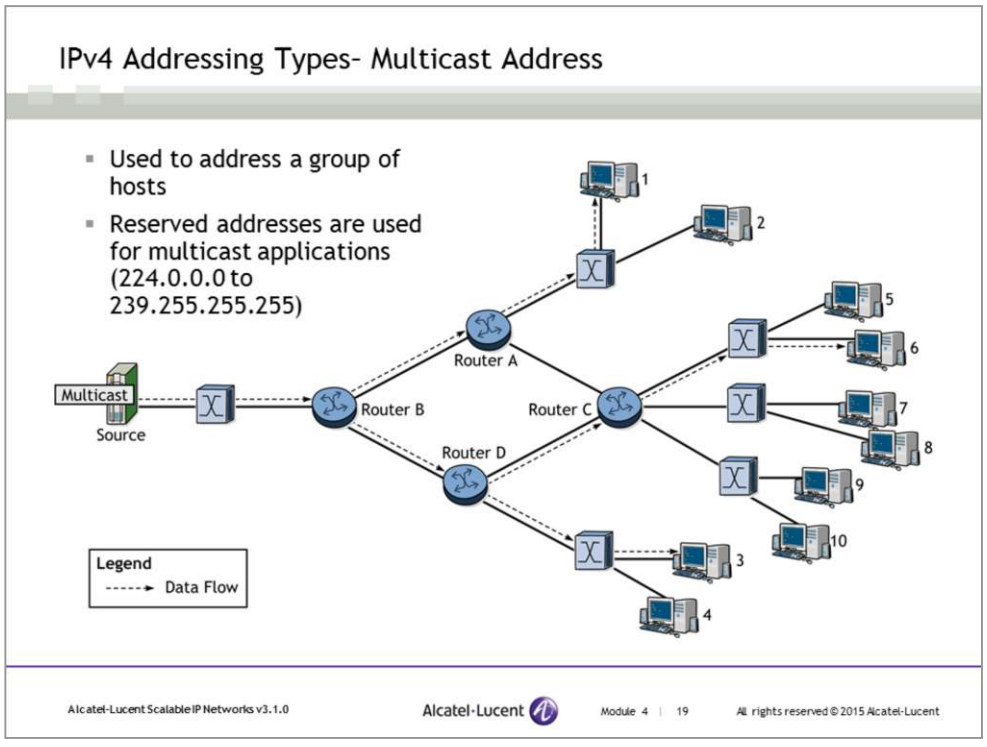


A broadcast address refers to all IP addresses in the broadcast domain. A packet sent from a source to all hosts in a broadcast domain is referred to as a broadcast packet. The destination IP address in a broadcast packet contains the network number and all 1s for the host address. For example, 138.120.255.255 specified in the destination IP header of a packet ensures that the packet will be delivered to all hosts in the 138.120.0.0 network. (The 255.255 section refers to all hosts.)

This slide shows a broadcast packet being flooded out to every host on the network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



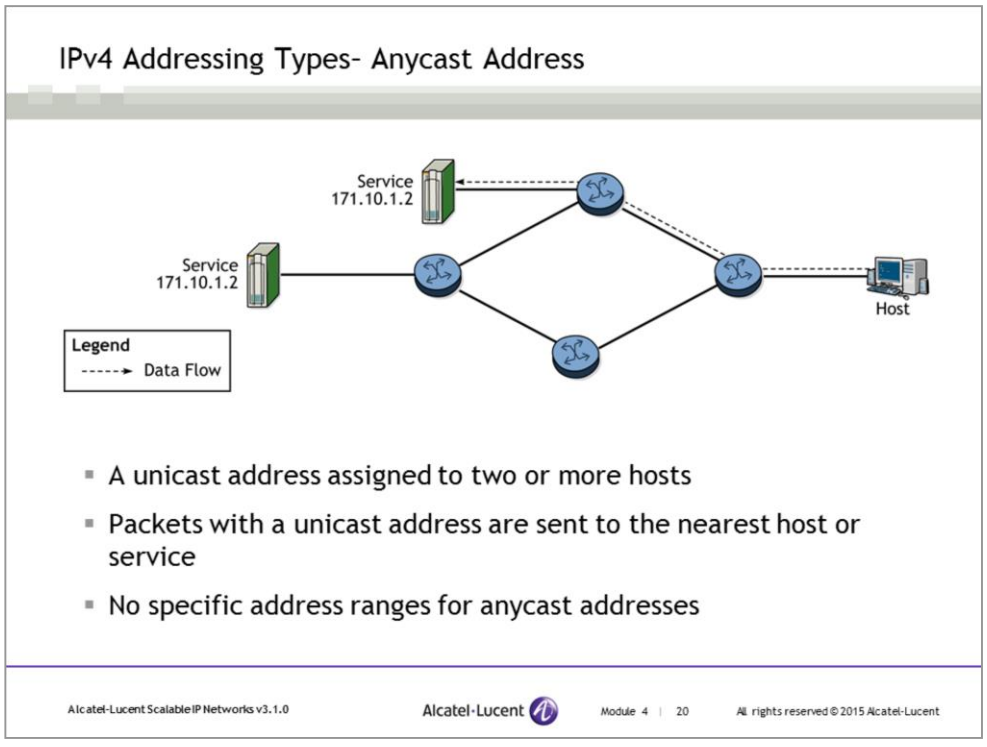
Multicast addresses are reserved for group membership applications. Multicast technology is an efficient way to deliver data to a group of destinations that need to receive the same data. The group of destinations is characterized by an IP address in the multicast range of 224.0.0.0 to 239.255.255.255 that defines membership in the specific group.

An example is a broadcast TV service. When a host wants to receive a specific channel, it uses a group membership protocol for that channel identified by a multicast range address, 239.1.1.1 for example. Multicast routing protocols route traffic from its source to the various hosts that require the traffic.

This slide shows how multicast packets can be forwarded to various hosts throughout the network. Each host is a member of a particular multicast group.

 All rights reserved © 2015 Alcatel-Lucent

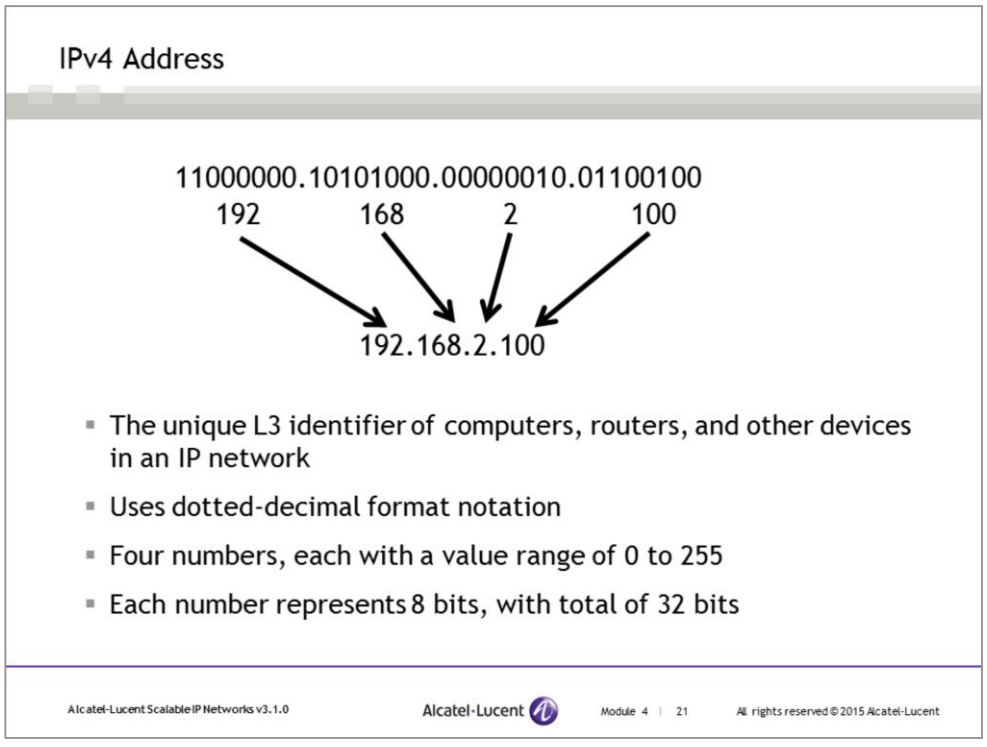
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



An anycast address is created by assigning the same unicast address to two or more hosts. In theory, the hosts are functionally equivalent, and packets should be routed to the nearest host. This works well in applications such as distributed websites. With the aid of dynamic routing protocols, the packets can find the nearest host and, if the host is not available, traffic is routed to the next-closest host.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



To make IPv4 addresses easier to read, they are expressed as four decimal numbers separated by a dot. This notation is called dotted-decimal notation.

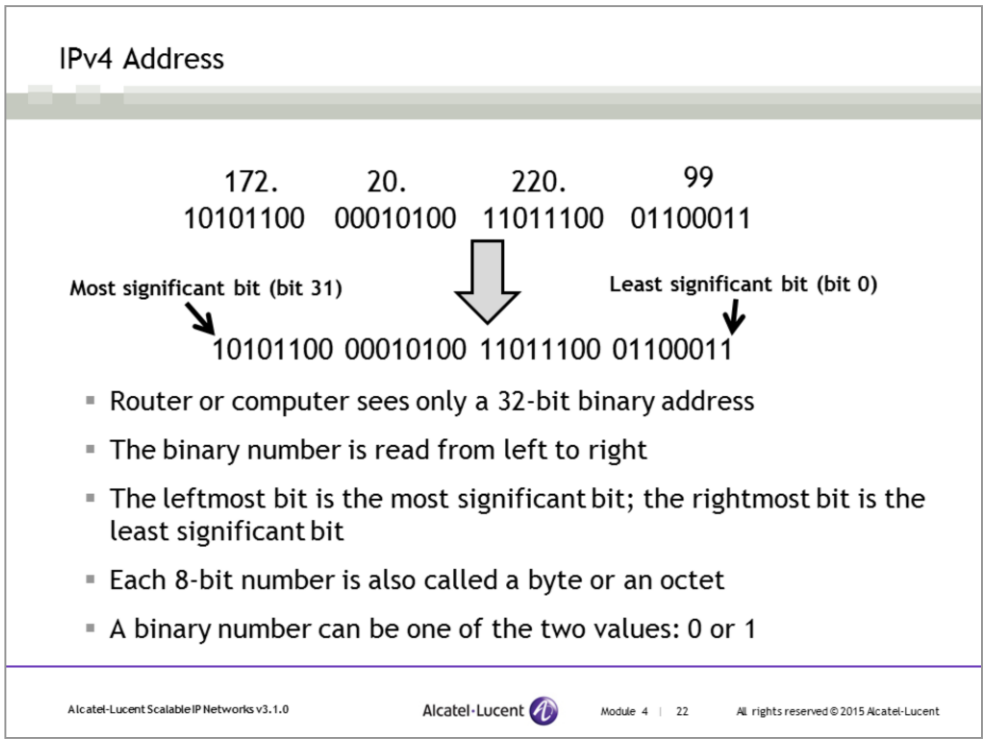
Dotted-decimal notation divides the 32-bit IP address into 4 bytes (octets) of 8 bits each. These octets specify the value of each field as a decimal number. The range of each octet is from 0 to 255 decimals or from 00000000 to 11111111 binary.

Neither the binary nor the decimal versions of the address are a single number, but rather four separate numbers separated by a dot (.). Each part of the binary number is 8 bits, for a total of a 32-bit address. In the binary number, each bit can only be a zero (0) or a one (1), equivalent to the "off" or "on" position of a circuit. To convert a binary number to decimal, raise the value 2 to the power of its position (0 to 7), multiple it by 0 or 1 (whichever bit is in that position), and then add the resulting numbers.

As stated earlier, the L3 address is unique to the device (except for anycast addresses) and, as such, is used to recognize the device on the Internet. This is analogous to the postal service. For you to receive mail that is meant for you and your family, you need a unique address. In Canada, the address is a combination of a postal code for a region, a street name, and a house number. For example, 123 Walden Drive, K2K 2S6 is a unique address in Canada. Similarly, every device that needs access to the Internet needs a unique L3 address.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

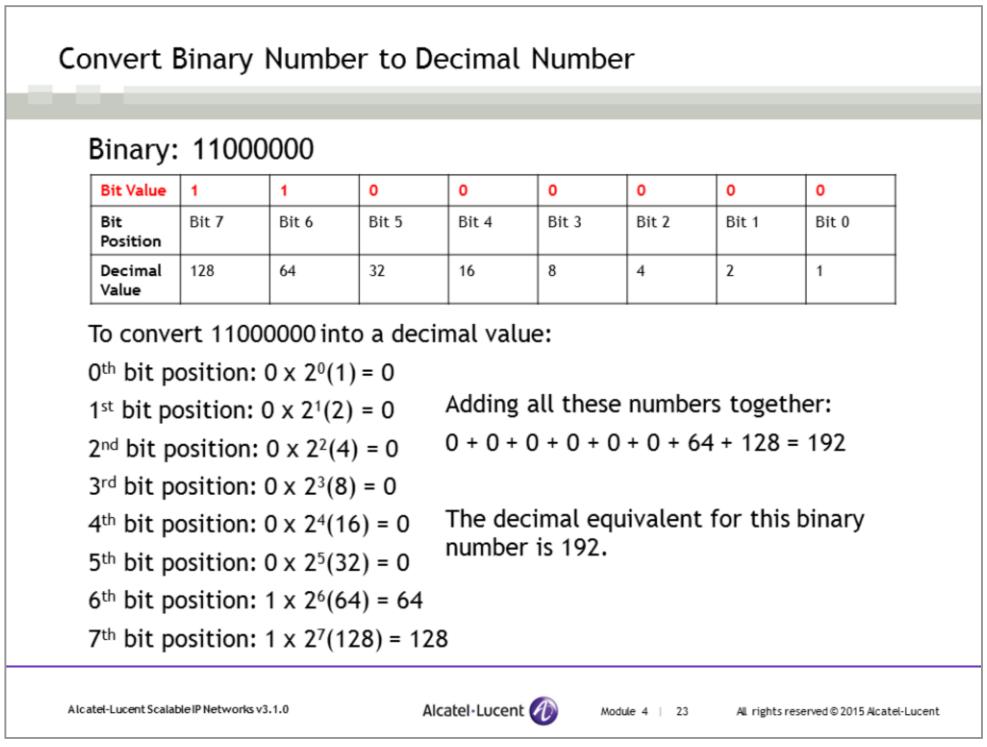


IPv4 addresses use a dotted-decimal notation. There are four numbers. Each number represents 8 bits, for a total of 32 bits.

Routers and/or computers only see a 32-bit binary address.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Let's demonstrate how to convert a binary number into a decimal number.

The binary number is 11000000. The numbers are read from right to left, with the rightmost bit being the lowest value (least significant bit) and the leftmost being the highest (most significant bit). To convert a binary number to decimal, take 0 or 1 (whichever bit is in that position), and multiply by the value 2 to the power of its position (0 to 7). Or you can make use of binary-to-decimal conversion table above.

The lowest position, or 0^{th} bit, has a value of 0. Multiply this by the value 2 to the power of 0 ($2^0 = 1$) equals 0

The next position, or 1^{st} bit, has a value of 0. Multiply this value by the value 2 to the power of 1 ($2^1 = 2$) equals 0

The next position, or 2^{nd} bit, has a value of 0. Multiply this value by the value 2 to the power of 2 ($2^2 = 4$) equals 0

The next position, or 3^{rd} bit, has a value of 0. Multiply this value by the value 2 to the power of 2 ($2^3 = 8$) equals 0

The next position, or 4^{th} bit, has a value of 0. Multiply this value by the value 2 to the power of 2 ($2^4 = 16$) equals 0

The next position, or 5^{th} bit, has a value of 0. Multiply this value by the value 2 to the power of 2 ($2^5 = 32$) equals 0

The next position, or 6^{th} bit, has a value of 1. Multiply this value by the value 2 to the power of 2 ($2^6 = 64$) equals 64

The next position, or 7^{th} bit, has a value of 1. Multiply this value by the value 2 to the power of 2 ($2^7 = 128$) equals 128

Adding all these numbers together, 0 + 0 + 0 + 0 + 0 + 0 + 64 + 128 = 192. Therefore, the decimal equivalent for the first of the four dotted-decimal numbers in the address is 192.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Exercise: Convert a binary address into a dotted-decimal address

Binary address: 11000000.10101000.00000010.01100100

Now, can you convert this binary address into a dotted-decimal address?

Very helpful to have a binary-to-decimal conversion table

Bit Position	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Decimal Value	128	64	32	16	8	4	2	1

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Exercise: Convert a binary address into a dotted-decimal address

Binary address: 11000000.10101000.00000010.01100100

Bit Position	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Decimal Value	128	64	32	16	8	4	2	1

1st octet: 11000000 => 128 + 64 = 192

2nd octet: 10101000 => 128 + 32 + 8 = 168

3rd octet: 00000010 => 2

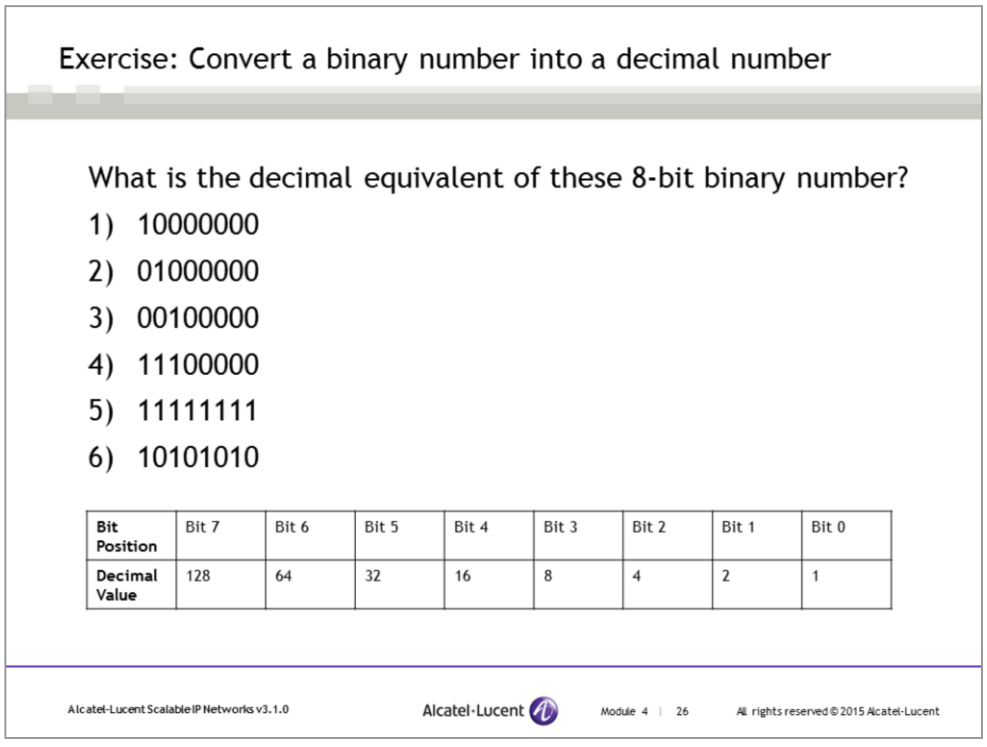
4th octet: 01100100 => 64 + 32 + 4 = 100

The dotted-decimal address is 192.168.2.100

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

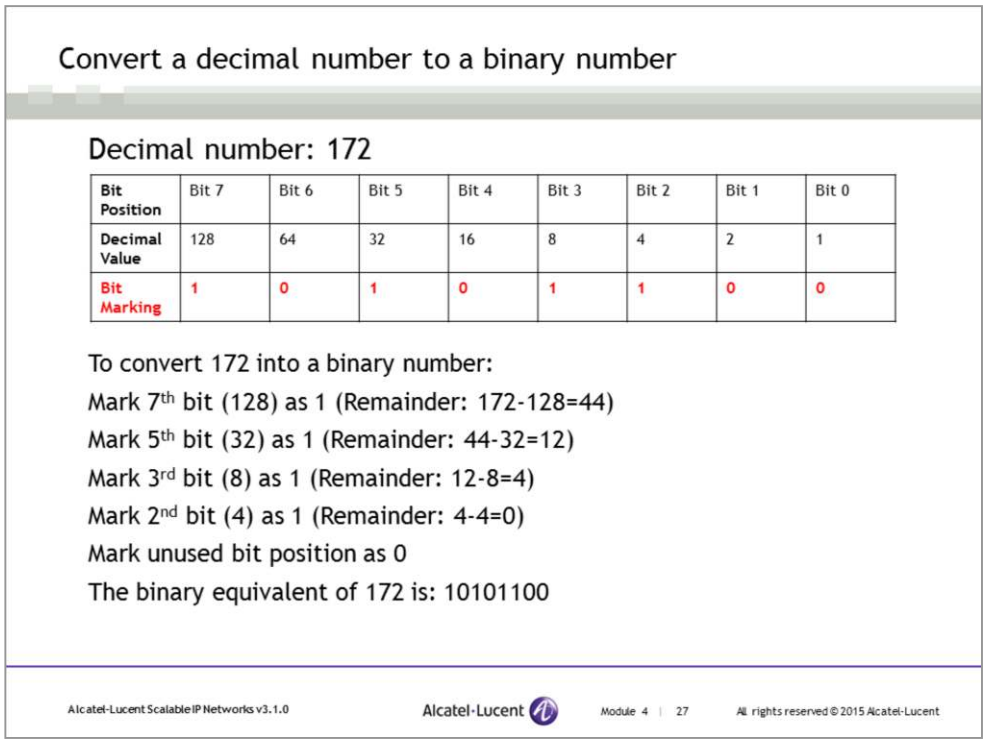


To convert a binary number to decimal, take 0 or 1 (whichever bit is in that position), multiply it by the value 2 to the power of its position (0 to 7) or simply use the binary-to-decimal conversion table.

1) 10000000 = 128
2) 01000000 = 64
3) 00100000 = 32
4) 11100000 = 128 + 64 + 32 = 224
5) 11111111 = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255 (if all bit positions have a value of 1, the decimal value is 255; if all bit positions have a value of 0, the decimal value is 0)
6) 10101010 = 128 + 32 + 8 + 2 = 170

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The process of converting a decimal number into a binary number is as follows:

1) Mark the highest (closest) bit position as 1

2) Subtract the corresponding bit value from the decimal value until there is no remainder

3) Mark any unused bit position as 0

To convert 172 to binary:

1. Mark 128 (bit 7) as 1. Remainder is 172 – 128 = 44
2. Mark 32 (bit 5) as 1. Remainder is 44 – 32 = 12
3. Mark 8 (bit 3) as 1. Remainder is 12 – 8 = 4
4. Mark 4 (bit 2) as 1. Remainder is 4 – 4 = 0
5. Mark unused bit positions as 0

The binary equivalent of 172 is 10101100.

To verify the binary conversion, convert the binary value back to a decimal value: 128+32+8+4=172.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Exercise: Convert a dotted-decimal address into a binary address

172.20.220.99

Can you convert this dotted-decimal address into a binary address?

Again, it is very helpful to have a binary-to-decimal conversion table

Bit Position	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Decimal Value	128	64	32	16	8	4	2	1

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Exercise: Convert a dotted-decimal address into a binary address

172.20.220.99

Bit Position	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Decimal Value	128	64	32	16	8	4	2	1
172	1	0	1	0	1	1	0	0
20	0	0	0	1	0	1	0	0
220	1	1	0	1	1	1	0	0
99	0	1	1	0	0	0	1	1

The binary address is 10101100 00010100 11011100 01100011

All rights reserved © 2015 Alcatel-Lucent

We know that the first octet 172 is binary 10101100.

To convert the second octet 20 to binary:

1. Mark 16 (bit 4) as 1. Remainder is 20 – 16 = 4
2. Mark 4 (bit 2) as 1. Remainder is 4 – 4 = 0
3. Mark any unused bit positions as 0

The binary equivalent of 20 is 00010100

To convert the third octet 220 to binary:

1. Mark 128 (bit 7) as 1. Remainder is 220 – 128 = 92
2. Mark 64 (bit 6) as 1. Remainder is 92 – 64 = 28
3. Mark 16 (bit 4) as 1. Remainder is 28 – 16 = 12
4. Mark 8 (bit 3) as 1. Remainder is 12 – 8 = 4
5. Mark 4 (bit 2) as 1. Remainder is 4 – 4 = 0
6. Mark any unused bit positions as 0

The binary equivalent of 220 is 11011100

To convert the forth octet 99 to binary:

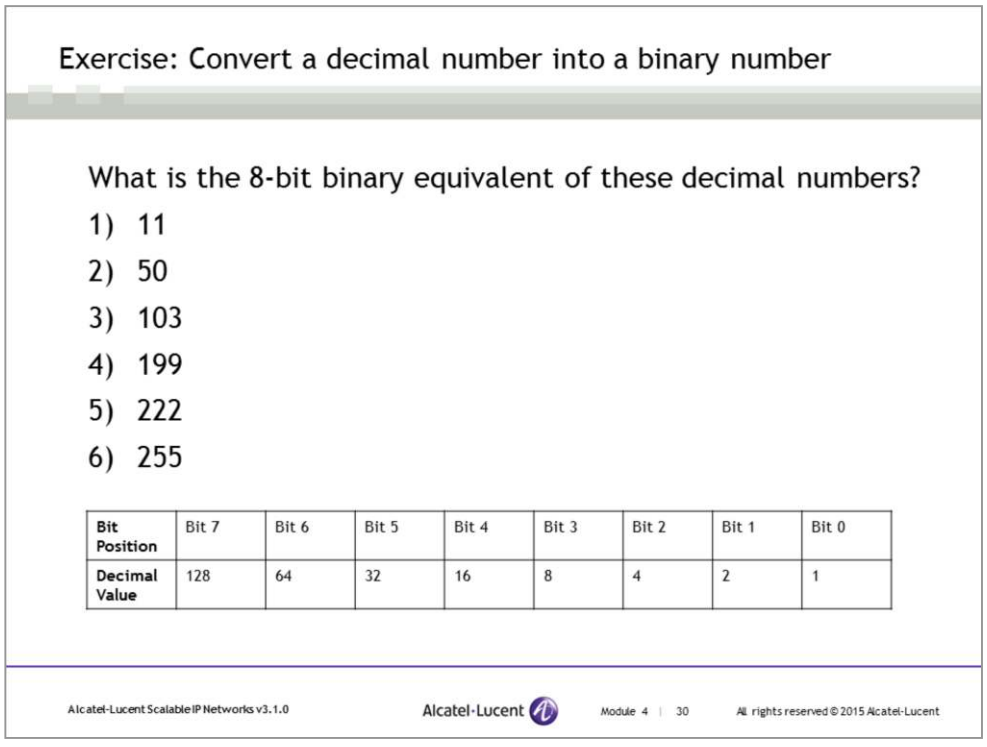
1. Mark 64 (bit 6) as 1. Remainder is 99 – 64 = 35
2. Mark 32 (bit 5) as 1. Remainder is 35– 32 = 3
3. Mark 2 (bit 1) as 1. Remainder is 3 – 2 = 1
4. Mark 1 (bit 0) as 1. Remainder is 1 – 1= 0
5. Mark any unused bit positions as 0

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

The binary equivalent of 99 is 01100011

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

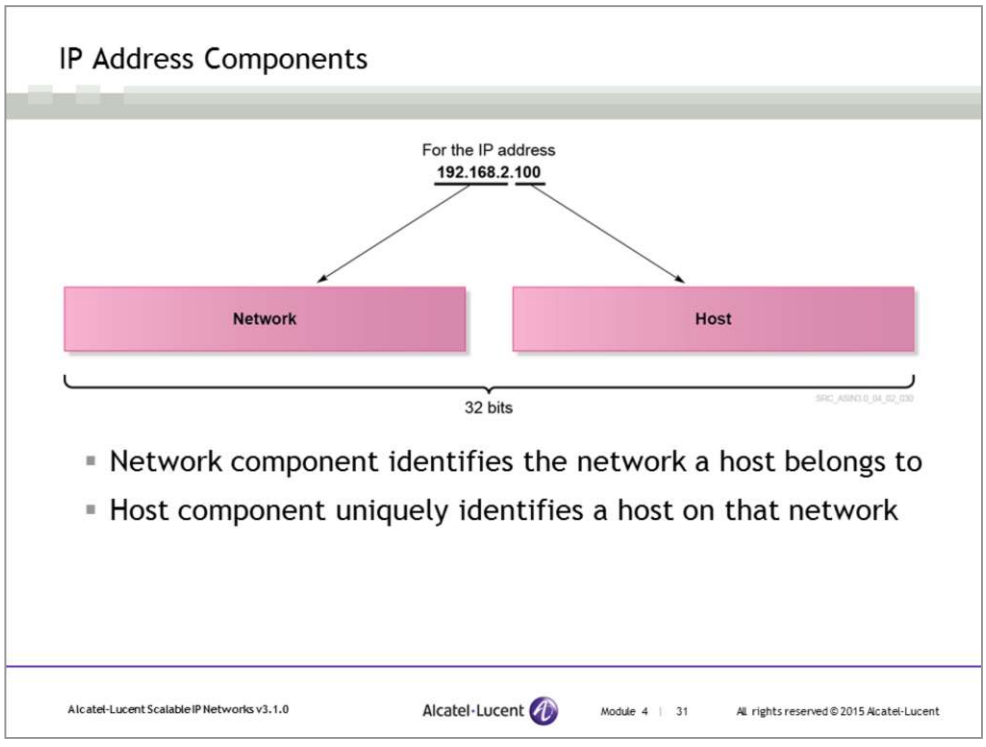


To convert a decimal number to binary, use the binary-to-decimal conversion table shown in the slide.

1) 11= 8 (bit 3) + 2 (bit 1) + 1 (bit 0) = 00001011
2) 50 = 32 (bit 5) + 16 (bit 4) + 2 (bit 1) = 00110010
3) 103 = 64 (bit 6) + 32 (bit 5) + 4 (bit 2) + 2 (bit 1) + 1 (bit 0) = 01100111
4) 199 = 128 (bit 7) + 64 (bit 6) + 4 (bit 2) + 2 (bit 1) + 1 (bit 0) = 11000111
5) 222 = 128 (bit 7) + 64 (bit 6) + 16 (bit 4) + 8 (bit 3) + 4 (bit 2) + 2 (bit 1) = 11011110
6) 255 = 128 (bit 7) + 64 (bit 6) + 32 (bit 5) + 16 (bit 4) + 8 (bit 3) + 4 (bit 2) + 2 (bit 1) + 1 (bit 0) = 11111111 (Note that 255 means all 8 bits are 1s)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



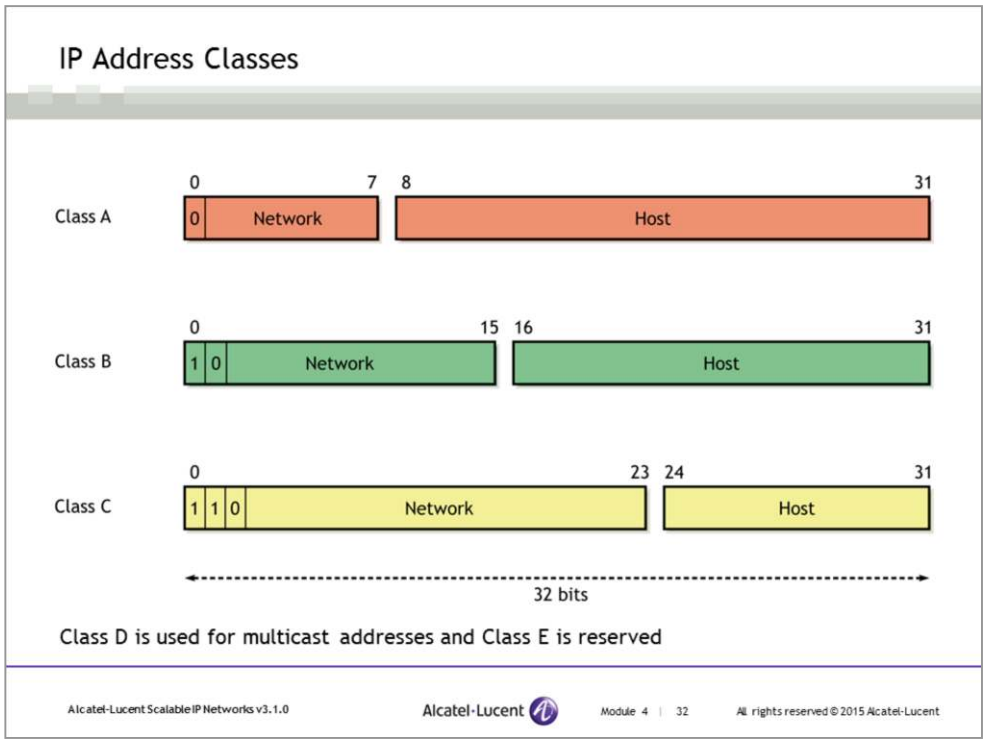
The first part of an IP address, known as the network component, identifies the network that a host resides in. This is similar to an area or country code for a phone number.

The second part of an IP address, known as the host component, uniquely identifies a host inside that network. This creates a two-level hierarchy, as shown in this slide.

All hosts in a network share the same network component. However, the host component must be unique to each host. Conversely, hosts with different network components may share the same host component. This is exactly like a phone number. Two people in the same area code cannot have the same phone number, but two people in different area codes can.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Original IPv4 networks used address classes to define the boundary between the network and host component. Early routing protocols did not include the subnet mask as part of the route update. However, Class C networks were too small for many networks, and Class A and Class B were too large for most networks, so this resulted in inefficient allocation of addresses. Original address allocation was not organized by geography at all – addresses were simply allocated sequentially based on network size.

In the early 1990s, Classless Inter-domain Routing (CIDR) was introduced to provide hierarchy in address allocation. Address class no longer had significance – the length of the network portion was determined by the subnet mask (or by prefix notation).

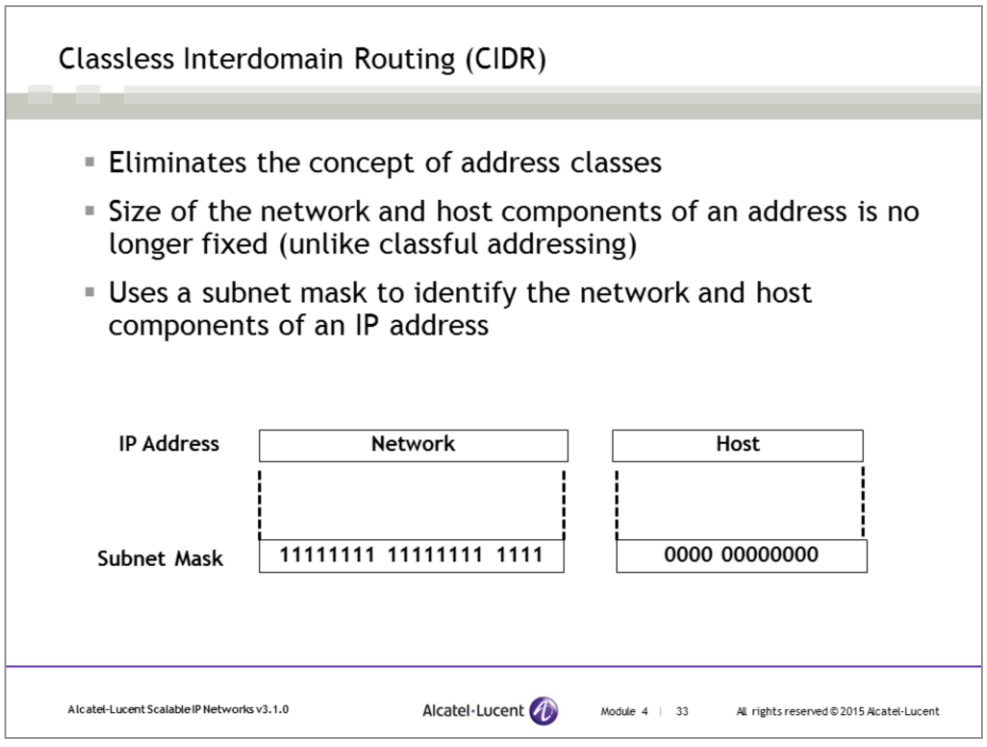
This division of addresses is referred to as *classful addressing* because the address space is split into predefined sizes. As shown in this slide, each class defines the boundary between the network and host at a different octet within the 32-bit address.

- Class A (1 to 126) — A Class A network has an 8-bit network prefix; the highest-order bit is always set to 0. Since 2 networks are always reserved, up to 126 networks can be defined. The 0.0.0.0 network is reserved for default routes. The 127.0.0.0 network is reserved for loopback functions.
- Class B (128 to 191) — A Class B network has a 16-bit network prefix; the two highest-order bits are always set to binary 10. Up to 16 384 networks can be defined.
- Class C (192 to 223) — A Class C network has a 24-bit network prefix and the three highest-order bits are always set to binary 110. Up to 2,097,152 networks can be defined.
- Class D (224 to 239) — Class D is used for multicast addresses in applications such as OSPF.
- Class E (240 to 255) — Class E is reserved.

Note that class-based addressing is obsolete and no longer relevant. Therefore, classful addressing will not be used or discussed for the remainder of this course.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



With the rapid expansion of the Internet, IPv4 addresses quickly became depleted, and the sizes of routing tables expanded exponentially. The response to these problems was the development and adaptation of Classless Interdomain Routing (CIDR).

CIDR eliminated the concept of address classes. Rather than the first 3 bits defining the network component, the subnet mask now defines the size of the network and host component.

Subnet mask is a 32-bit number that uses the same dotted-decimal notation as an IP address. In binary, the subnet mask contains a sequence of ones, followed by a sequence of zeroes.

The bits that are 1 in the subnet mask represent the bits corresponding to the network component.

The bits that are 0 in the subnet mask represent the bits corresponding to the host component.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

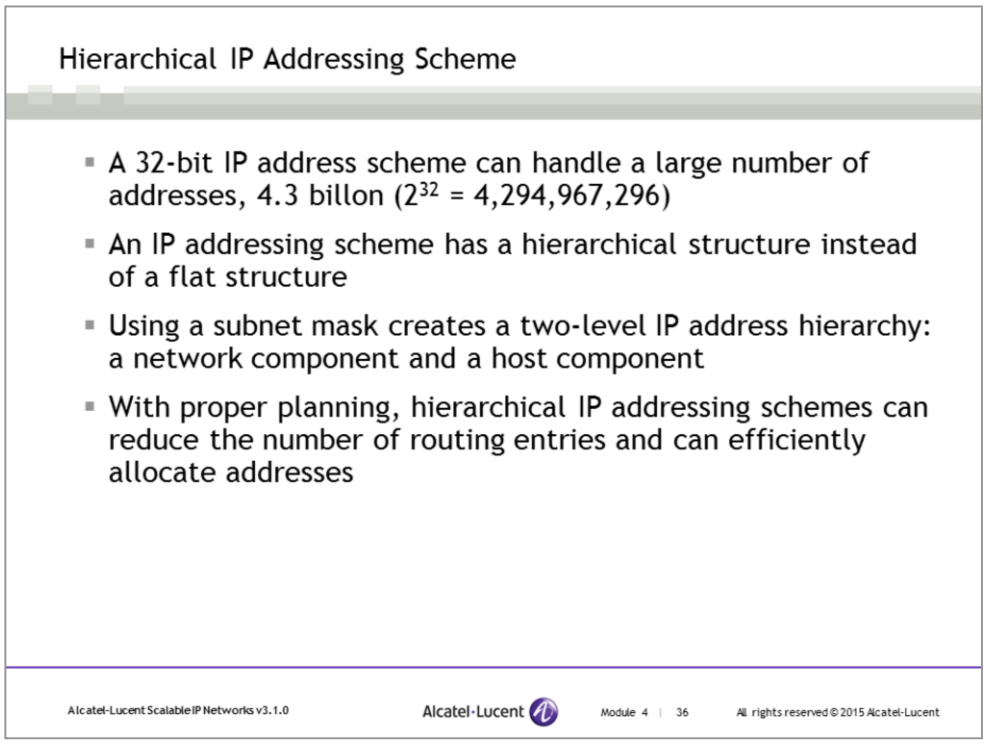
After successful completion of this section, you will be able to:

- Explain the importance of hierarchy in IPv4 addressing
- Describe how hierarchy is accomplished using the subnet mask (host and network component)
- Describe how subnetting is used to divide a network into smaller subnets
- Describe how subnet addresses can be summarized at network boundaries

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 4 | 35
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

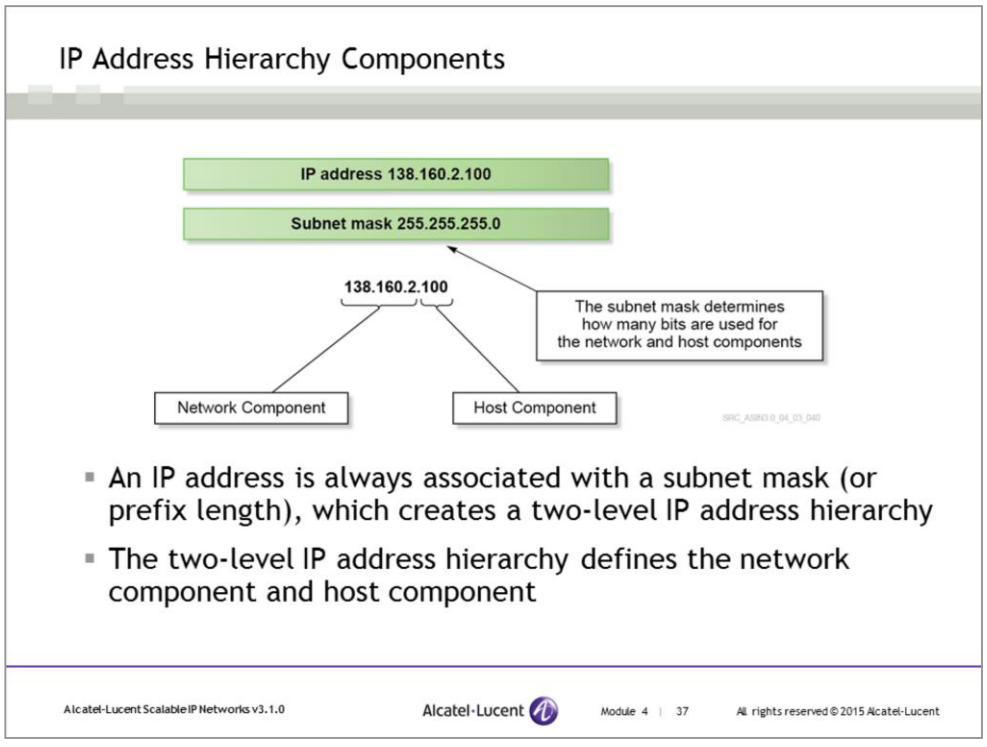


An IP address scheme makes use of a hierarchical structure comprised of network components and host components. A network component identifies the network that a host resides in. A host component identifies a host in the network.

In a hierarchical IP addressing scheme, a single network can be used to represent multiple networks and therefore reduce the number of routing entries in the routers. This concept is called aggregation or summarization. Also, IP addresses can be efficiently allocated using variable length subnet mask (VLSM). A subnet mask can be of different lengths, based on the address allocation requirement, and is no longer limited by address classes.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



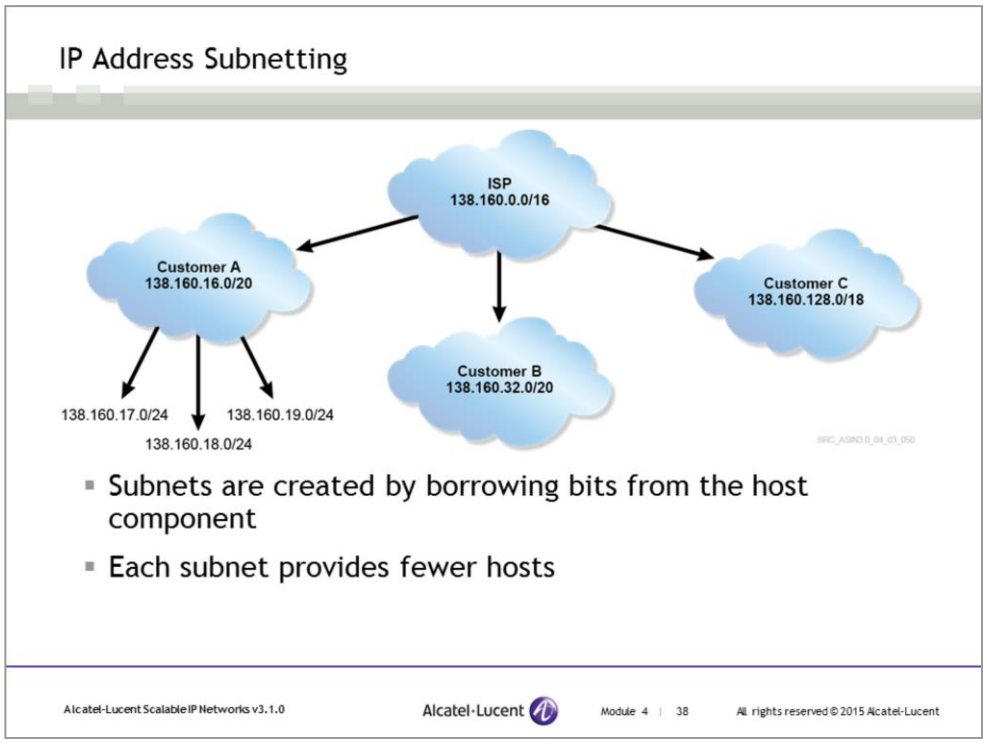
An IP address is always associated with a subnet mask or prefix length. This provides a two-level address hierarchy. The first part of an IP address is the network component, or network prefix, and the second part of an IP address is the host component.

In this slide, an IP address of 138.160.2.100/24 has a subnet mask of 255.255.255.0 (24 bits of 1s followed by 8 bits of 0s). This means that the first 24 bits are used for the network component, and the remaining 8 bits are used for the host component. More details about subnet masks will be discussed in the next section. For now, you just need to know that the two-level IP address hierarchy defines two components: the network component and the host component.

As mentioned earlier, all hosts in a network share the same network number. However, the host numbers must be unique to each host. Conversely, hosts with different network prefixes may share the same host number. A network component identifies the network that a host resides in, similar to an area code or country code for a phone number. A host component identifies a host in the network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IP subnetting is used to create additional sub-networks (subnets) from a single network, with each subnet providing for fewer hosts. Essentially, a portion of the addresses are borrowed from the host component and given to the network component. ISPs typically use subnetting to create subnets for their customers.

In this example, an Internet Service Provider (ISP) has a network of 138.160.0.0/16. This means that the first 16 bits are used for the network prefix and the remaining 16 bits are used for the host addresses. The ISP assigns three smaller subnets to its customers, Customers A, B, and C, using subnetting. The ISP can decide on how many bits to borrow from its network's host addresses and make them part of the network prefix for the subnets.

Customer A has a subnet of 138.160.16.0/20. The first 20 bits are used for the network component (4 bits are borrowed from the host component of 138.160.0.0/16), and the remaining 12 bits are used for the host component for the new subnet.

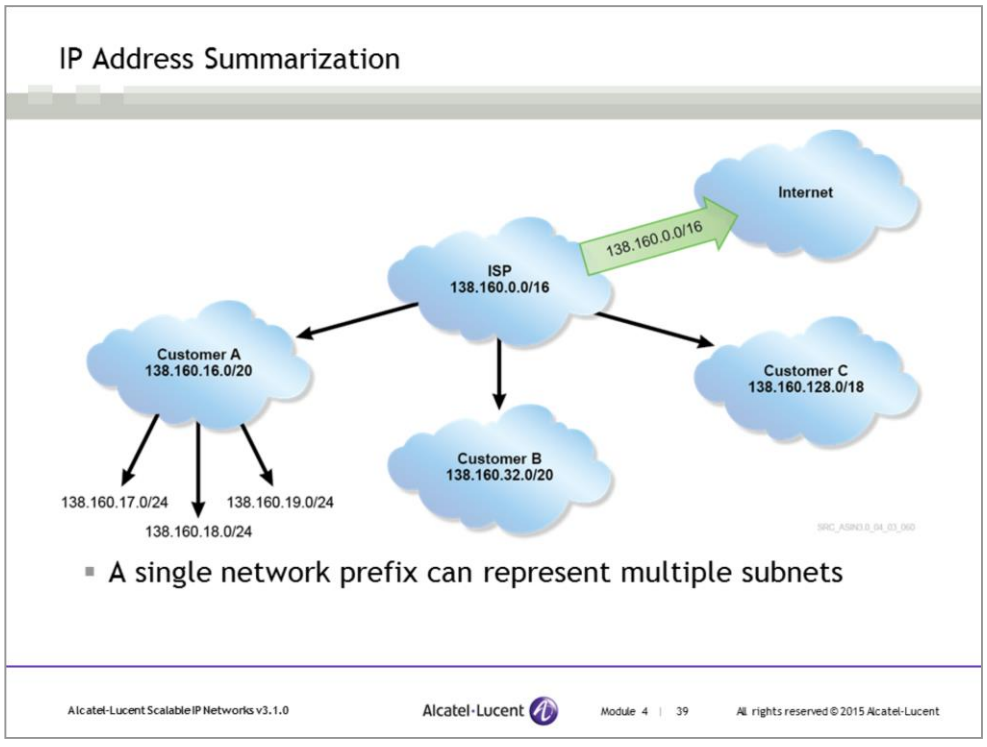
Customer B has a subnet of 138.160.32.0/20. The first 20 bits are used for the network component (4 bits are borrowed from the host component of 138.160.0.0/16), and the remaining 12 bits are used for the host component for the new subnet.

Customer C has a subnet of 138.160.128.0/18. The first 18 bits are used for the network prefix (2 bits are borrowed from the host component of 138.160.0.0/16), and the remaining 14 bits are used for the host component for the new subnet.

Similar to how the ISP assigns subnets to its customers, Customer A can be an ISP reseller and assign additional subnets by borrowing four bits from its host component of 138.160.16.0/20 and using them for the new subnets' network component.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IP address summarization allows a single route entry to represent multiple networks. When summarization or aggregation is applied, all subnets can be represented by as few entries as possible in the routing table. As the Internet grows, more and more entries are required for routers to handle the routing of IP datagrams, which causes performance problems for routers.

In this slide, the ISP advertises only one route to the Internet, 138.160.0.0/16, for all its customers. The rest of the Internet does not need to know the details of the ISP's customers. Instead of advertising all subnets to the Internet, the IP address summarization improves routing efficiency and stability.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

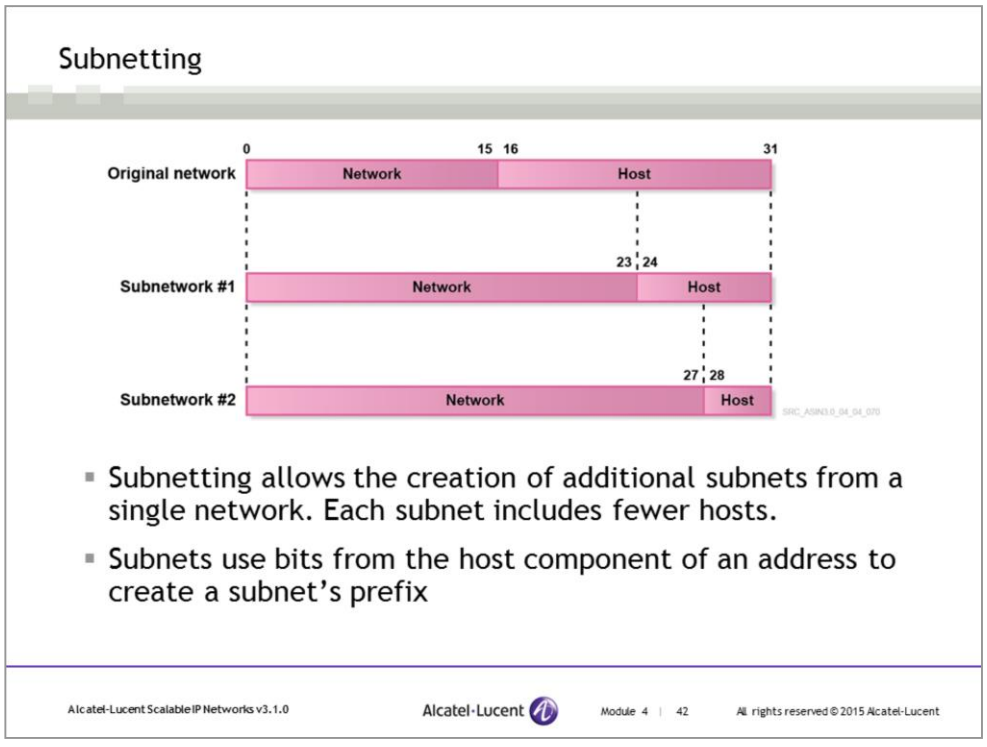
After successful completion of this section, you will be able to:

- Explain the function of a subnet mask
- Calculate possible host addresses and broadcast address from a given IP address and subnet mask
- Identify steps on how to create a subnet address plan based on customer requirements
- Describe the characteristics of the two types of router interfaces
- Describe the functions of the special subnet masks
- Describe how to configure and verify a router interface

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



An IP address is always associated with a subnet mask or prefix length. This provides a two-level address hierarchy. The first part of an IP address is the network component, or network prefix, and the second part of an IP address is host component.

Subnetting allows for the creation of more subnets within a single network. In order to subnet a network, a subnet mask is extended using some of the bits from the host component of an address to create the network component of a new subnet.

In this example, the original network has 16 bits used for the network portion and another 16 bits used for the host portion. With 16 bits used for host addresses, there can be up to 65,536 (2^{16}) hosts on this network.

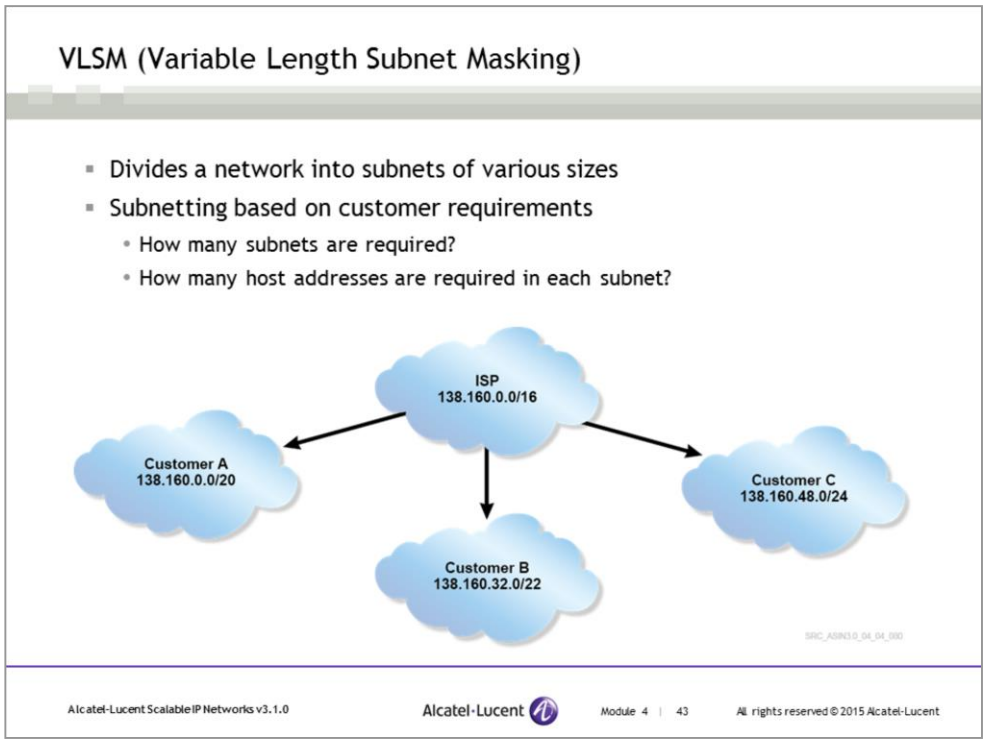
Subnetwork #1 is created by borrowing bits from the host portion of the original network and giving them to the network portion of network #2. Therefore, in subnetwork #1 twenty-four bits are used for the network portion, and the remaining 8 bits are used for the host portion. With 8 bits used for host addresses, there can be up to 256 (2^8) hosts on this network.

Similarly, subnetwork #2 is created by borrowing bits from the host portion of subnetwork #1 and giving them to the network portion of subnetwork #2. Therefore, in subnetwork #2 twenty-eight bits are used for the network portion, and the remaining 4 bits are used for the host portion. With 4 bits used for host addresses, there can only be up to 16 (2^4) hosts on this network.

As each network/subnet is created, a smaller number of hosts is available.

All rights reserved © 2015 Alcatel-Lucent

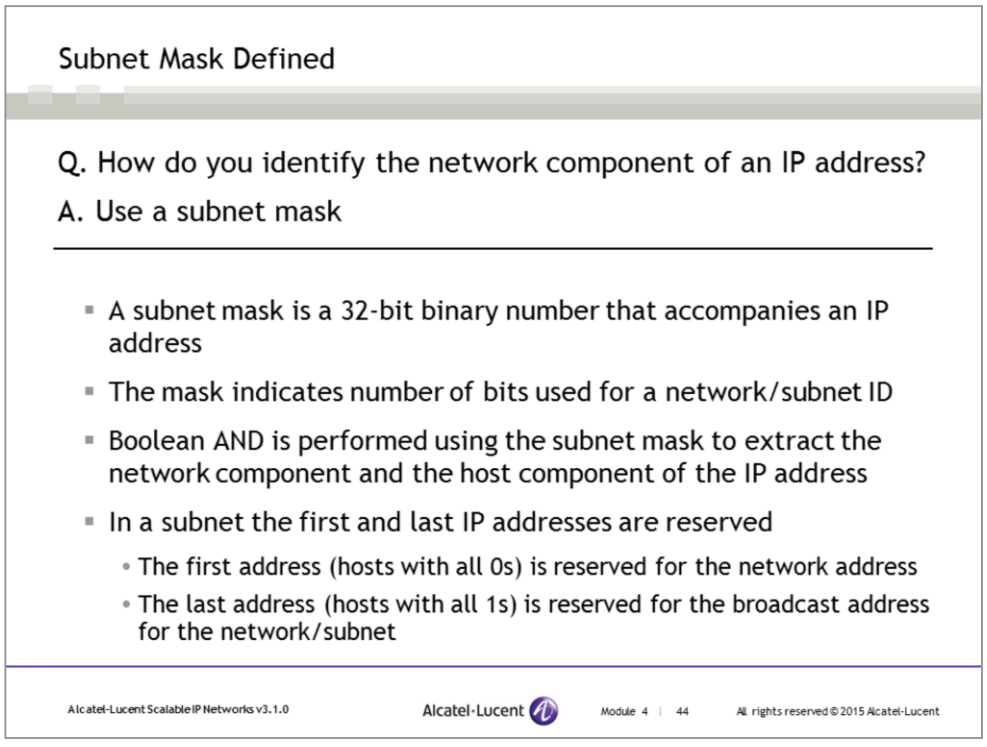
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



VLSM allows a network to be divided into subnets of various sizes. Subnets that need more host addresses can have a different subnet mask than the subnets that need less host addresses.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

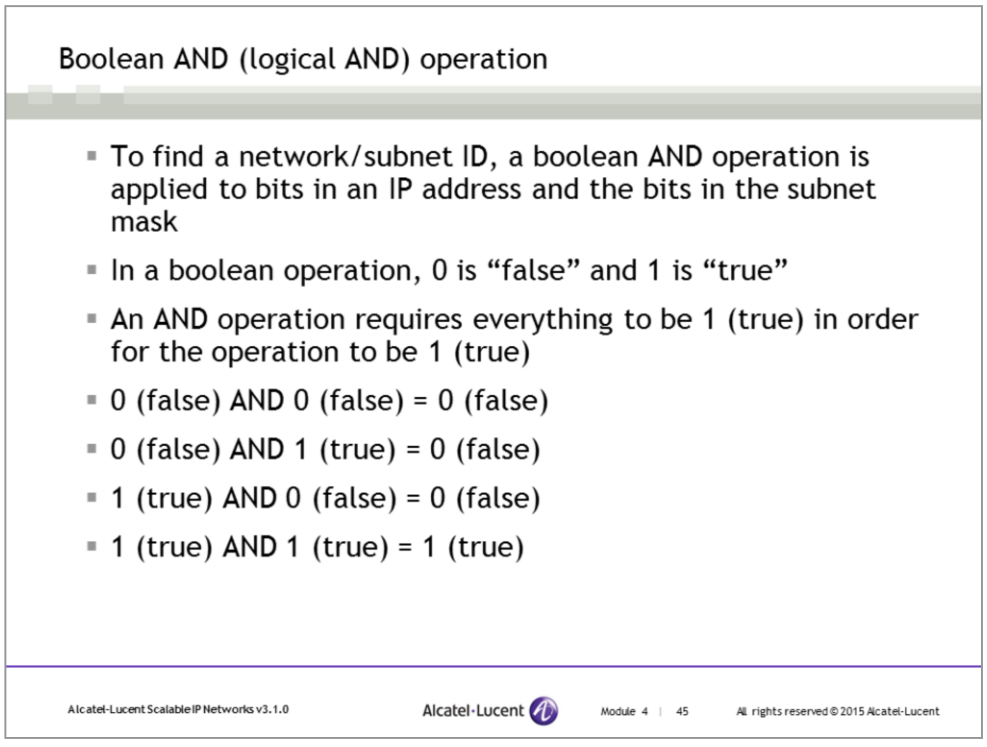


A subnet mask is a 32-bit binary number that consists of a sequence of 1s followed by a sequence of 0s. The subnet mask is created so that it has 1 bit for each corresponding bit of the IP address that is part of its network ID or subnet ID, and a 0 bit for each bit of the IP address's host ID. Essentially, a binary 1 in the mask represents the network portion, and a binary 0 represents the host portion. Therefore, the mask tells TCP/IP devices which bits in the IP address belong to the network ID and subnet ID, and which bits in the IP address are part of the host ID.

A router performs a logical AND operation between a destination address and the subnet mask to derive the network portion of the address. This leaves the network portion unchanged and makes the host portion all zeroes.

 All rights reserved © 2015 Alcatel-Lucent

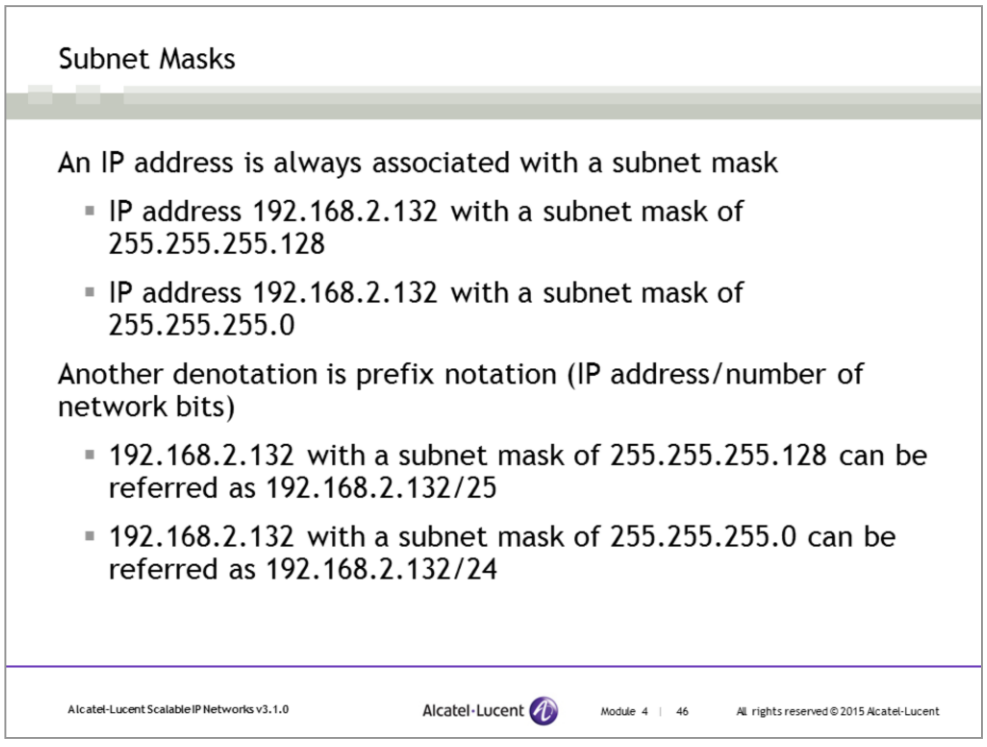
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A Boolean operation is simply a logical operation, such as an AND or OR. In a Boolean operation, you can think of a 0 as “false” and a 1 as “true”. An AND operation requires everything to be 1 (true) in order for the operation to be 1 (true).

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



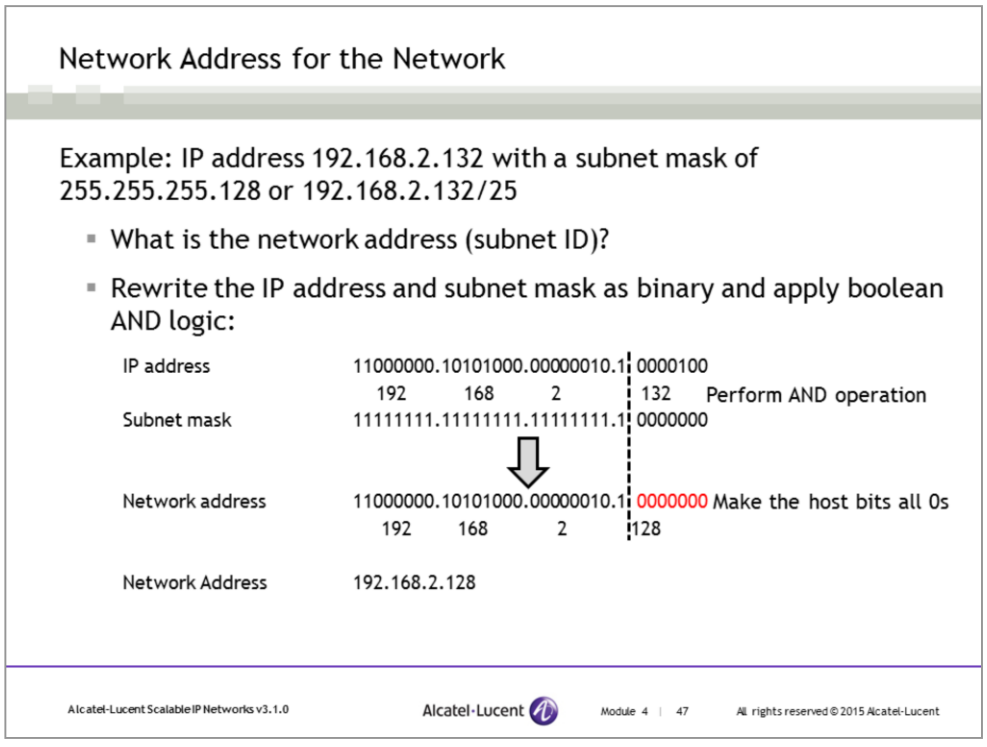
The use of a number to indicate the mask is much less cumbersome than writing out the address and is a very common representation of an IP address and its associated mask. People will often refer to these as “24-bit mask” or “16-bit mask”. The number here is sometimes called prefix length. Using this decimal shortcut is fine, provided you understand how this number was derived from the binary.

All possible subnet masks and prefix length are as follows:

128.0.0.0	/1	255.255.128.0	/17
192.0.0.0	/2	255.255.192.0	/18
224.0.0.0	/3	255.255.224.0	/19
240.0.0.0	/4	255.255.240.0	/20
248.0.0.0	/5	255.255.248.0	/21
252.0.0.0	/6	255.255.252.0	/22
254.0.0.0	/7	255.255.254.0	/23
255.0.0.0	/8	255.255.255.0	/24
255.128.0.0	/9	255.255.255.128	/25
255.192.0.0	/10	255.255.255.192	/26
255.224.0.0	/11	255.255.255.224	/27
255.240.0.0	/12	255.255.255.240	/28
255.248.0.0	/13	255.255.255.248	/29
255.252.0.0	/14	255.255.255.252	/30
255.254.0.0	/15	255.255.255.254	/31
255.255.0.0	/16		

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A subnet mask is used to determine the host portion of an address. Note that 255 means “all 1s” in binary.

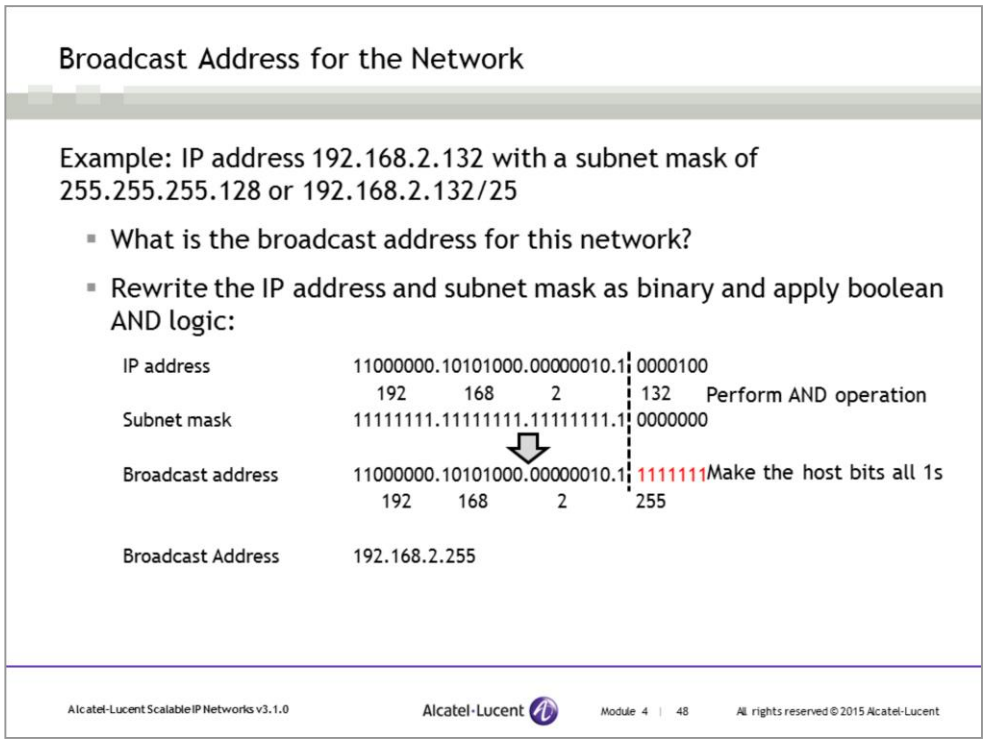
This example: 192.168.2.132 with a subnet mask of 255.255.255.128.

Before applying the AND operation, it is much easier to write the IP address and subnet mask in binary form. The subnet mask of 255.255.255.128 (11111111.11111111.11111111.10000000) contains 25 bits of 1s and 7 bits of 0s. This means that the first 25 bits of the IP address are used for the network portion and the last 7 bits are used for the host portion. The first 25 bits of the IP address with the last 7 bits set to zero is the network address for this IP address. To determine the network address (also called a subnet ID), the subnet mask of 255.255.255.128 (11111111.11111111.11111111.10000000) is applied to the IP address of 192.168.2.132 (11000000.10101000.00000010.100000100) using an AND operation. The network address is therefore 192.168.2.128 (11000000.10101000.00000010.10000000).

The network address is the lowest address on the network, where host bits are all zeroes.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Every IP network has a network address and a broadcast address for the network. The network address is the lowest address on the network (host bits are all zeroes). The broadcast address is the highest address on the network (host bits are all ones).

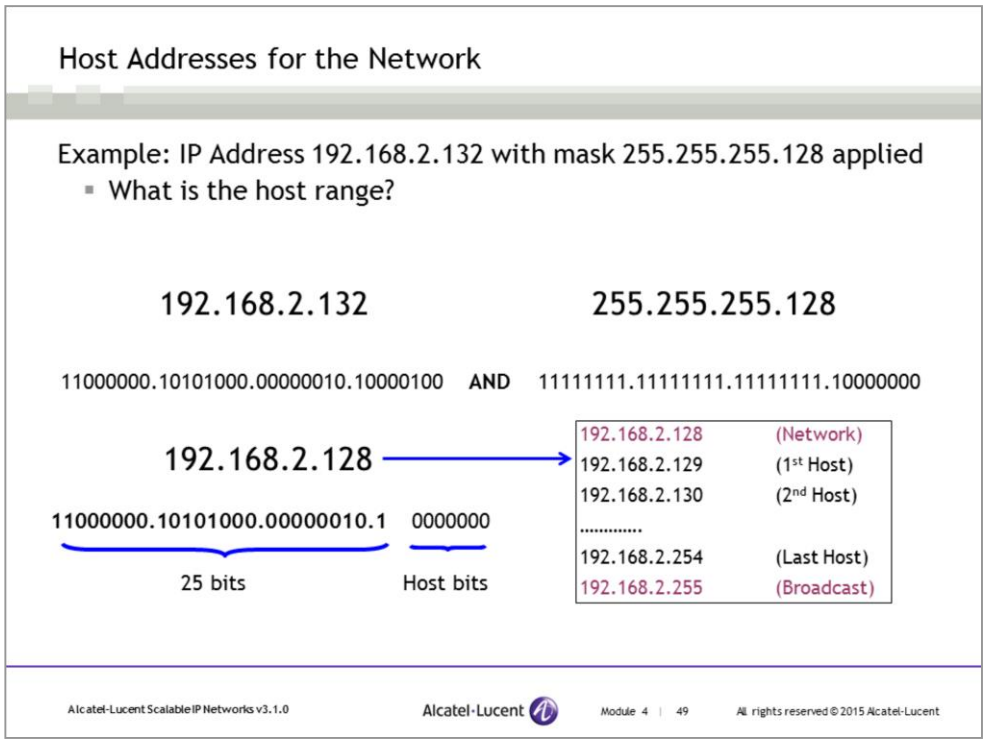
Network and broadcast addresses are reserved and cannot be assigned to a host. All numbers between the network and broadcast addresses can be assigned to hosts.

In this example, there are 7 bits for the host component. Each bit has two possible values (0 or 1). The number of hosts available is $2^7 = 128$. To calculate the number of hosts available, use the formula 2^n, where n is the number of bits available.

The address with host bits of all zeroes is a network address; the address with host bits of all ones is a broadcast address. These two addresses are reserved. The number of available hosts that can be assigned on this network is $2^7 - 2 = 126$.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The address with host bits of all zeroes is a network address for the network; the address with host bits of all ones is a broadcast address for the network.

For the network 192.168.2.128 (11000000.10101000.00000010.10000000):

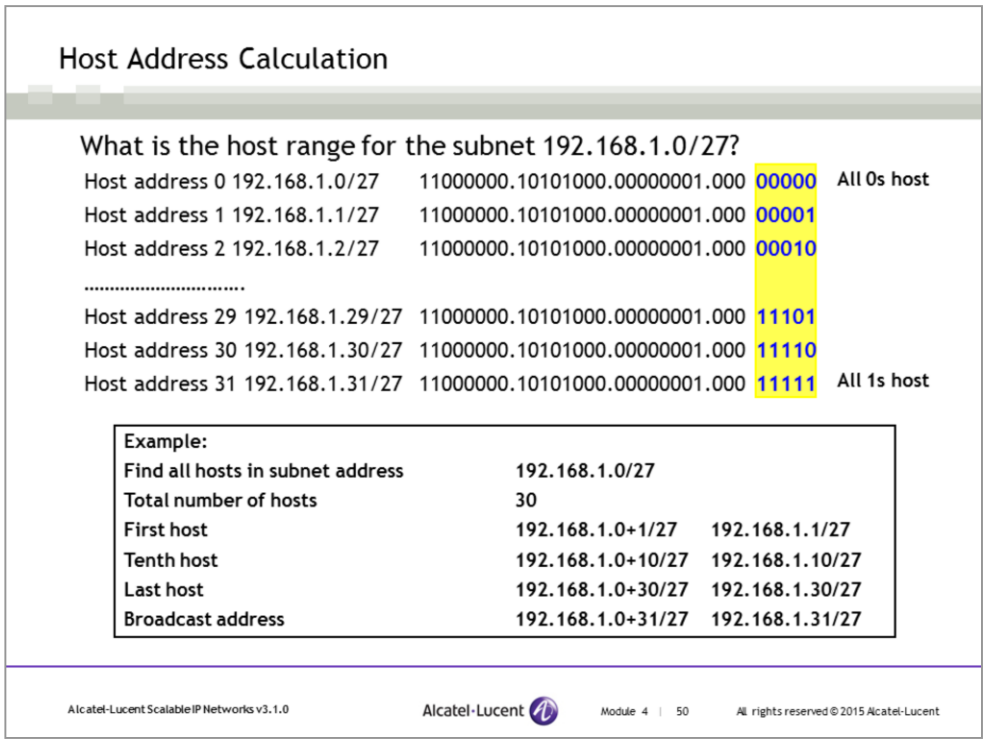
The network address has all 7 host bits set to 0s, which equals to 192.168.2.128 (11000000.10101000.00000010.10000000) and cannot be used for a host.

The broadcast address has all 7 host bits set to 1s, which equals to 192.168.2.255 (11000000.10101000.00000010.11111111) and cannot be used for a host.

The host address range is from 129 (10000001) up to 254 (11111110).

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



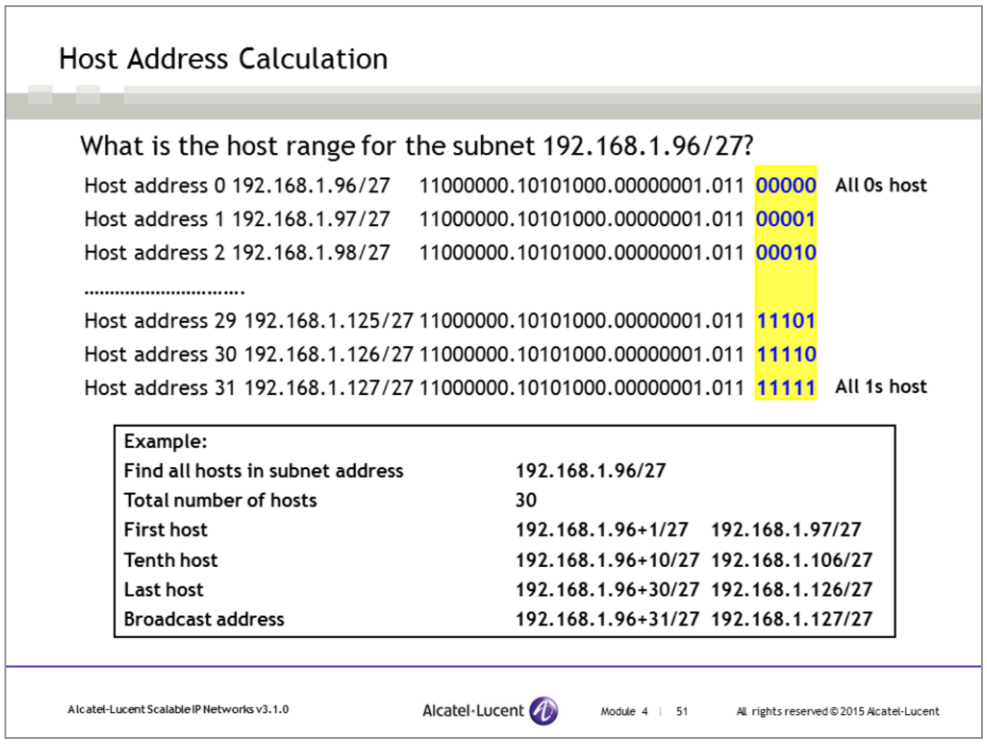
The assigned host address field of a network cannot contain all zeroes or all ones. The host number of all zeroes is reserved for the network address; the host number of all ones is reserved for the broadcast address for the network or subnet.

For address 192.168.1.0/27:

- 27 bits are used for the network portion because the subnet mask is /27.
- The remaining 5 bits (32 – 27) are used for the host addresses.
- Using the formula of 2^5 -2 = 32 -2 = 30, there are 30 assignable host addresses in this subnet. This means that this subnet can support up to 30 hosts.
- To define the host address for the tenth host in the subnet, arrange the host bits in the bit pattern that represents 10 or 01010. This is then added to the network address of 192.168.1.0/27 to give a host address of 192.168.1.10/27.
- To define the broadcast address for this subnet, the host bits would be all set to 1 or 11111. This is the binary representation of 31, or 31 would be added to the network address of 192.168.1.0/27 to give a broadcast address of 192.168.1.31/27 for this subnet.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

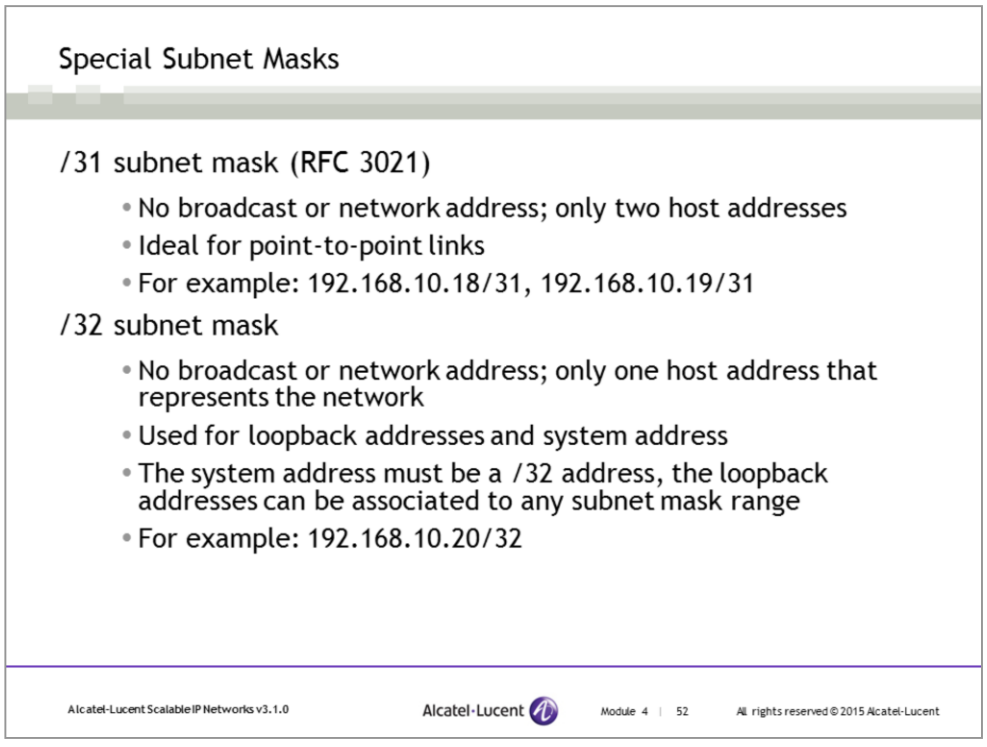


For address 192.168.1.96/27:

- 27 bits are used for the network portion because the subnet mask is /27.
- The remaining 5 bits (32 – 27) are used for the host addresses.
- Using the formula of 2^5 -2 = 32 -2 = 30, there are 30 assignable host addresses in this subnet. This means that this subnet can support up to 30 hosts.
- To define the host address for the tenth host in the subnet, you arrange the host bits in the bit pattern that represents 10 or 01010. This is then added to the network address of 192.168.1.96/27 to give a host address of 192.168.1.106/27.
- To define the broadcast address for this subnet, the host bits would be all set to 1 or 11111. This is the binary representation of 31, or 31 would be added to the network address of 192.168.1.96/27 to give a broadcast address of 192.168.1.127/27 for this subnet.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



/31 subnet mask

- Using the example of 192.168.10.18/31 in the classical sense decodes to a subnet mask of 255.255.255.254 with a network address of 192.168.10.18 and a broadcast address of 192.168.10.19.
- Because no addresses are reserved for host spaces, the devices need to be able to handle the addresses as two host addresses and not as broadcast/network addresses.

/32 subnet mask

- There is only one address reserved for loopback addresses and the system address.
- The system address is a special loopback address that serves as a router ID for routing protocols such as OSPF and BGP.
- Loopback addresses are internal logical addresses that are not associated with physical interfaces.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Choosing a Subnet Mask

- Based on number of hosts required
- Select the next highest power of two
- Same method is used to determine the number of bits needed to create subnets

Number of Hosts Required	Round up to the next power of two	Prefix Length	Subnet Mask
10	$2^4 = 16$	/28 (32-4)	255.255.255.240
50	$2^6 = 64$	/26 (32-6)	255.255.255.192
100	$2^7 = 128$	/25 (32-7)	255.255.255.128
400	$2^9 = 512$	/23 (32-9)	255.255.254.0
1000	$2^{10} = 1024$	/22 (32-10)	255.255.252.0

 All rights reserved © 2015 Alcatel-Lucent

The subnet mask is usually chosen based on the number of hosts that need to be supported on the network.

1) Take the number of hosts required and round up to the nearest power of two. This will be the number of bits that will be used for the host portion of a network.
2) Find the number of bits used for the network portion (number of bits for the network portion = total number of bits in an IP address (32) – number of bits for the host portion).
3) The subnet mask contains a sequence of ones, followed by a sequence of zeros. The bits that are 1 in the subnet mask represent the bits corresponding to the network component. The bits that are 0 in the subnet mask represent the bits corresponding to the host component.

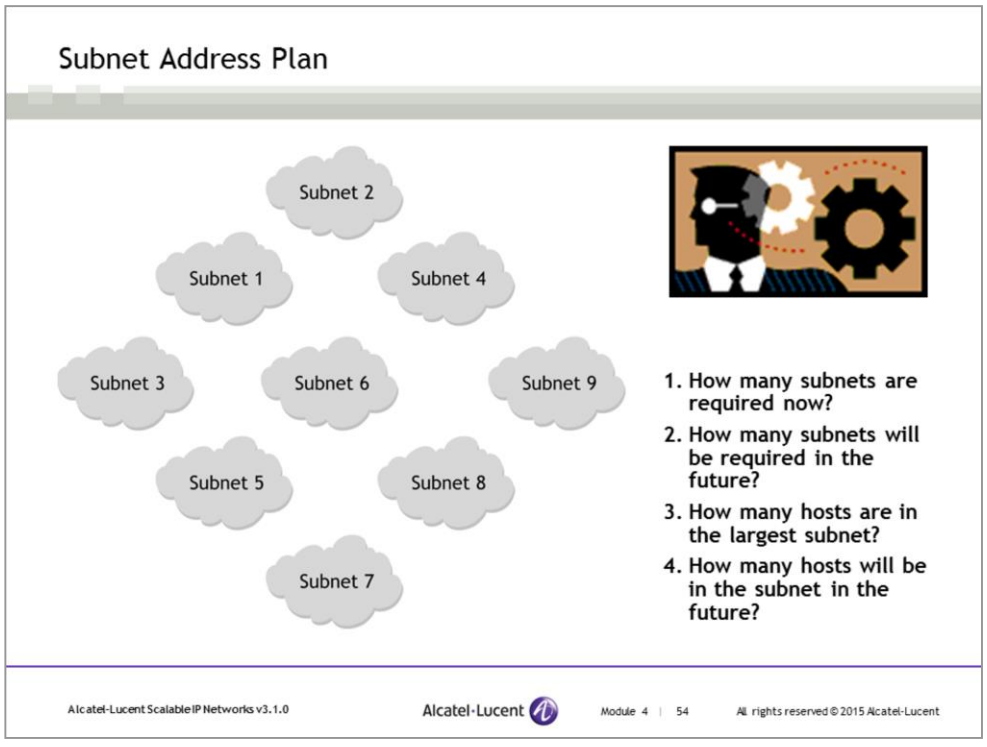
For example, if the number of hosts required is 10, the next power of two is 2^4=16. The number of bits used for the network portion (prefix length) is 32-4=28. The subnet mask contains a sequence of 28 ones, followed by a sequence of 4 zeros. Therefore, the subnet mask is 11111111 11111111 11111111 11110000 or 255.255.255.240.

A similar method is used to calculate the number of bits to be borrowed from a network for the new subnet's network component. The number of bits to be borrowed depends on the number of subnets required.

If 5 subnets are required, 2^3 = 8, or 3 bits, are borrowed from a network for the new subnet's network component.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



An addressing plan requires careful preparation and consideration for future requirements. The network administrator cannot just look at the existing infrastructure in the assignment of addresses but must also consider the future growth of hosts in all subnets, and the future growth in the number of subnets that will be required.

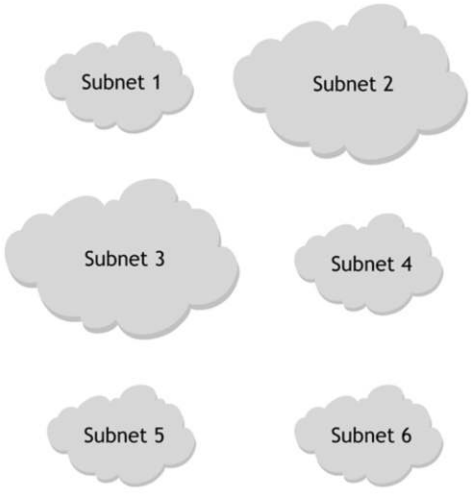
To create a subnet address plan, the administrator must perform the following steps:

1. Define the number of subnets required.
   In this slide, there is a requirement for nine subnets; Using 3 host bits to create 2^3 or 8 subnets would not meet the requirement. To meet this requirement, the administrator must use 4 host bits to create 2^4 = 16 subnets. This now leaves room for future expansion.
2. Ensure there is enough host space available to meet the requirements of the largest subnet. If the largest subnet requires 35 hosts, a 2^6 = 64 host space must be used. 6 bits must be reserved for the hosts. This size also leaves room for expansion because there can be up to 64 – 2 = 62 hosts for each subnet, which is more than the required 35 hosts.
3. After the design is completed, ensure that the organization's allocated IP address space is sufficient to meet current and future needs.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Subnet Address Plan - Example

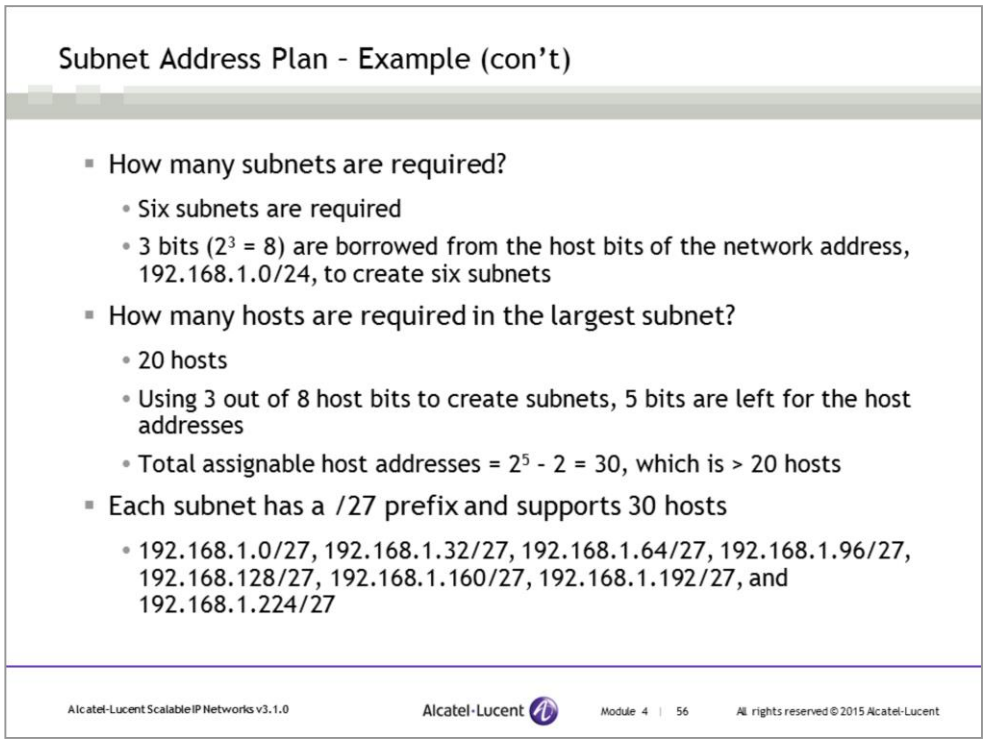


1. Subnet 2, the largest subnet, requires 20 host addresses
2. Network IP address is 192.168.1.0/24

 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The administrator must identify the bits needed to provide the six required subnets. Because the address is a binary address, the boundaries for the subnets are based on the power of two.

In this slide, the administrator requires 3 bits of the existing host bits of the network address to provide the necessary subnets: 2^3 = 8 available subnets. This gives the subnets a prefix of 27 bits. The 4-octet subnet mask appears as 255.255.255.224 (the binary equivalent would be 11111111.11111111.11111111.11100000). Notice how the last octet in binary clearly shows the 3 bits from the host bits of the network address to create the needed subnets.

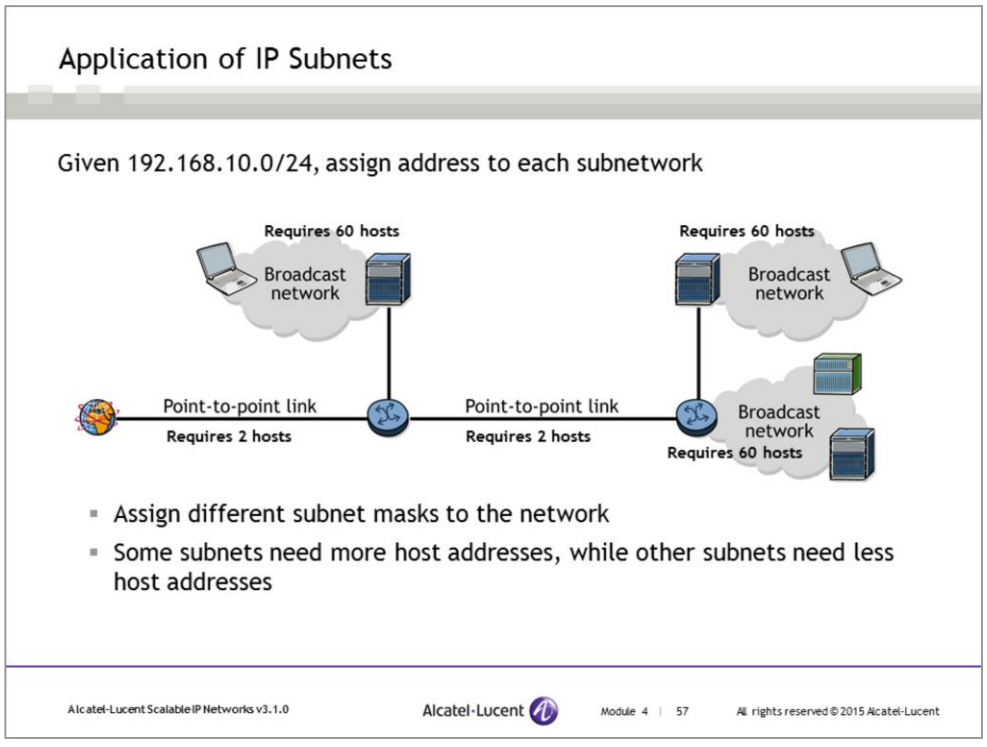
Using 3 out of 8 bits to create subnets leaves 5 bits of the last octet for host addresses. The calculation for usable or assignable host addresses is 2^n – 2, or in this case 2^5 – 2. Two host addresses must be subtracted from the total because the host address 00000 (all 0s) is reserved for the network address and the host address of 11111 (all 1s) is reserved for the broadcast address of the subnet.

The network address is 192.168.1.0/24. With the subnet extended prefix defined, the administrator has the following subnets, with each subnet supporting 30 hosts:

192.168.1.0/27
192.168.1.32/27
192.168.1.64/27
192.168.1.96/27
192.168.1.128/27
192.168.1.160/27
192.168.1.192/27
192.168.1.224/27

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



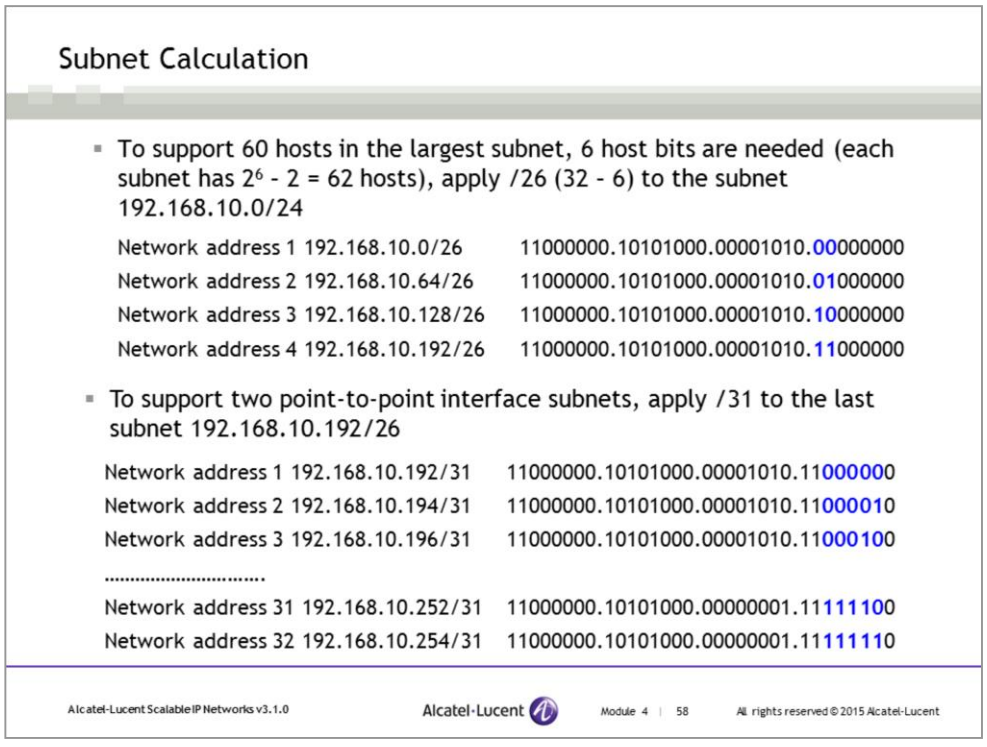
Some subnets may require more host addresses, while other subnets may require less host addresses.

If the networks are spread over a number of different sites, the administrator must ensure that enough bits are used to support the current sites and any future sites that may be deployed. In addition, the administrator must envision how each site may further subdivide the network to support the subnetworks in each site.

Development of this hierarchical addressing scheme requires careful consideration and planning. The network must recursively work its way down so that each level has enough space in the host address to support each requirement.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Apply /26 to the subnet 192.168.10.0/24, two bits (32 – 24 – 6 = 2) are used for network/subnet portion, and therefore four subnets are created ($2^2 = 4$).

192.168.10.0/26 (last octet is binary **00**000000)

192.168.10.64/26 (last octet is binary **01**000000)

192.168.10.128/26 (last octet is binary **10**000000)

192.168.10.192/26 (last octet is binary **11**000000)

Apply /31 to the last subnet 192.168.10.192/26 to support point-to-point interface subnets.

192.168.10.192/31 (last octet is binary 11**00000**0)

192.168.10.194/31 (last octet is binary 11**00001**0)

192.168.10.196/31 (last octet is binary 11**00010**0)

192.168.10.198/31 (last octet is binary 11**00011**0)

192.168.10.200/31 (last octet is binary 11**00100**0)

:

192.168.10.252/31 (last octet is binary 11**11110**0)

192.168.10.254/31 (last octet is binary 11**11111**0)

The last two /31 subnets can be used to represent the two point-to-point links.

 All rights reserved © 2015 Alcatel-Lucent

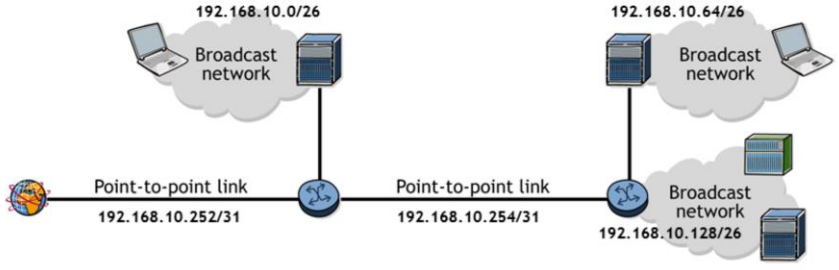
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Subnet Assignment

Different subnet masks are applied to different subnets in the network depending on the number of hosts required in each subnet

Each broadcast network requiring 60 hosts has a /26 subnet

Each point-to-point link requiring 2 hosts has a /31 subnet



 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

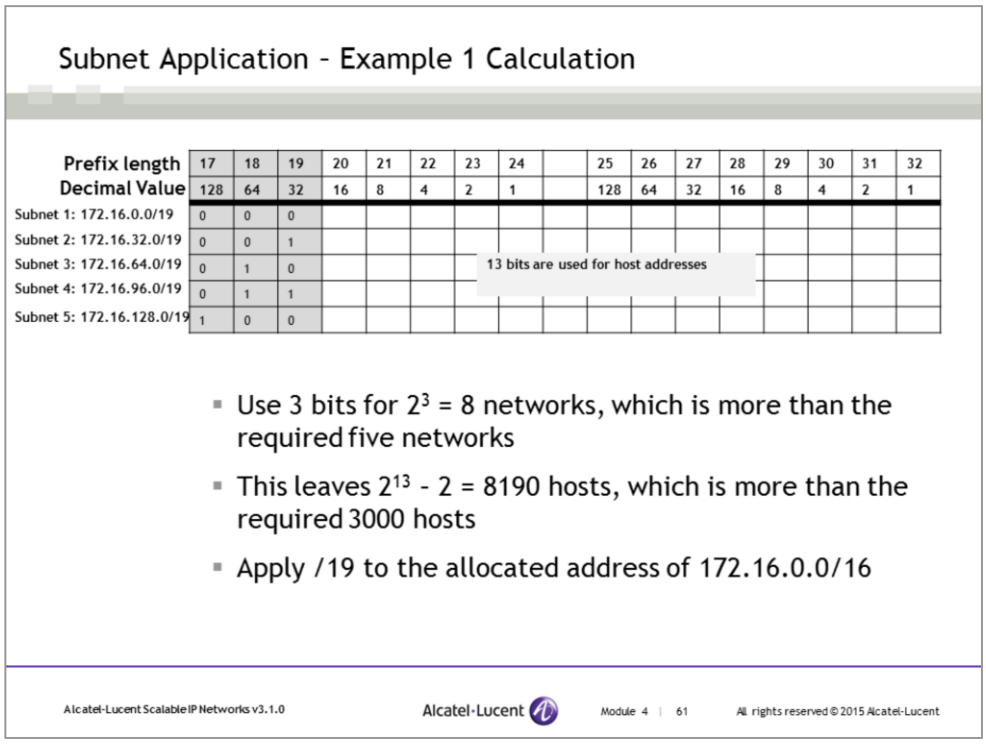
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Subnet Application - Example 1

- In this example, the service provider is allocated an IP address of 172.16.0.0/16
- The organization requires five subnets
- All subnets require at least 3000 hosts

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The last 16 bits can be used to subnet the network 172.16.0.0/16. We need five networks. To obtain the required networks, use 3 bits out of 16 for 2^3 = 8 networks and 2^{13} = 8192 hosts. 8192 hosts is more than the 3000 hosts required by the largest subnets. However, if the largest subnet is expected to grow with no more than 4000 hosts in any subnet, more host bits will be required.

Using 3 network bits, 13 host bits are used (2^{13} = 8192) for host addresses in the subnets. Apply /19 (32 – 13) to the subnet 172.16.0.0/16, the following network addresses are available:

172.16.0.0/19 (third octet is binary **000**00000)

172.16.32.0/19 (third octet is binary **001**00000)

172.16.64.0/19 (third octet is binary **010**00000)

172.16.96.0/19 (third octet is binary **011**00000)

172.16.128.0/19 (third octet is binary **100**00000)

172.16.160.0/19 (third octet is binary **101**00000)

172.16.192.0/19 (third octet is binary **110**00000)

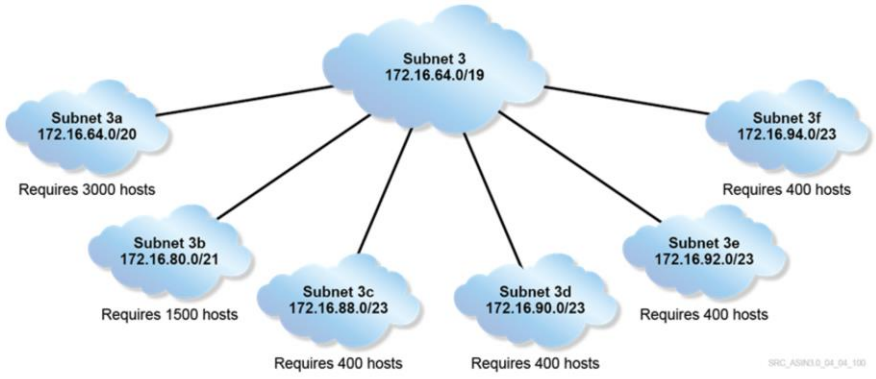
172.16.224.0/19 (third octet is binary **111**00000)

The first five network addresses can be used for the five subnets. Subnet 1, 2, 3, 4, and 5 are assigned with subnets 172.16.0.0/19, 172.16.32.0/19, 172.16.64.0/19, 172.16.96.0/19 , and 172.16.128.0/19, respectively.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Subnet Application - Example 2

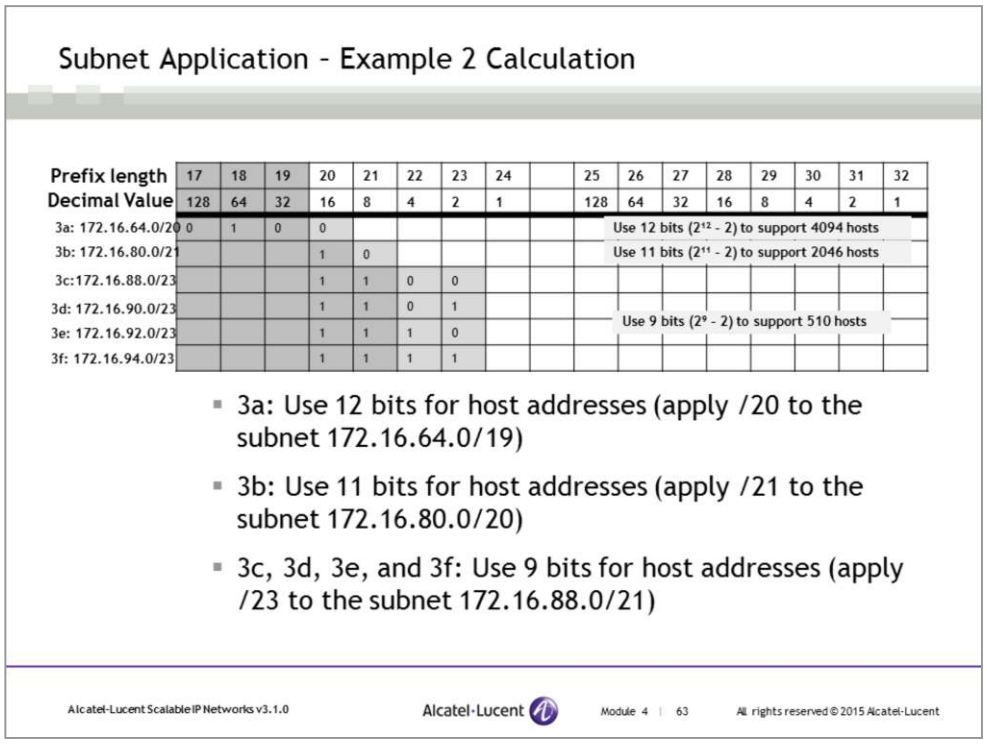


A subnet 172.16.64.0/19 must be further subnetted into 6 subnets that support different numbers of hosts

 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, subnet 172.16.64.0/19 has been isolated and will be further subdivided to support the six subnets that are located in the local campus. The total number of hosts supported in the /19 network is $2^{(32-19)} - 2 = 8190$. This can be further subdivided into more subnetworks, each with a smaller number of hosts.

There are many options. One of the options is as follows:

Subnet 3a: Use 12 bits out of 13 (32 - 19) for $2^{12} - 2 = 4094$ hosts, which is more than the required 3000 hosts. Therefore, subnet 3a can be assigned 172.16.64.0/20 with 4094 hosts available.

The remaining subnet 172.16.80.0/20 can be further divided for other smaller subnets.

Subnet 3b: Use 11 bits out of 12 (32 - 20) for $2^{11} - 2 = 2046$ hosts, which is more than the required 1500 hosts. Therefore, subnet 3b can be assigned 172.16.80.0/21 with 2046 hosts available.

The remaining subnet 172.16.88.0/21 can be further divided for other smaller subnets.

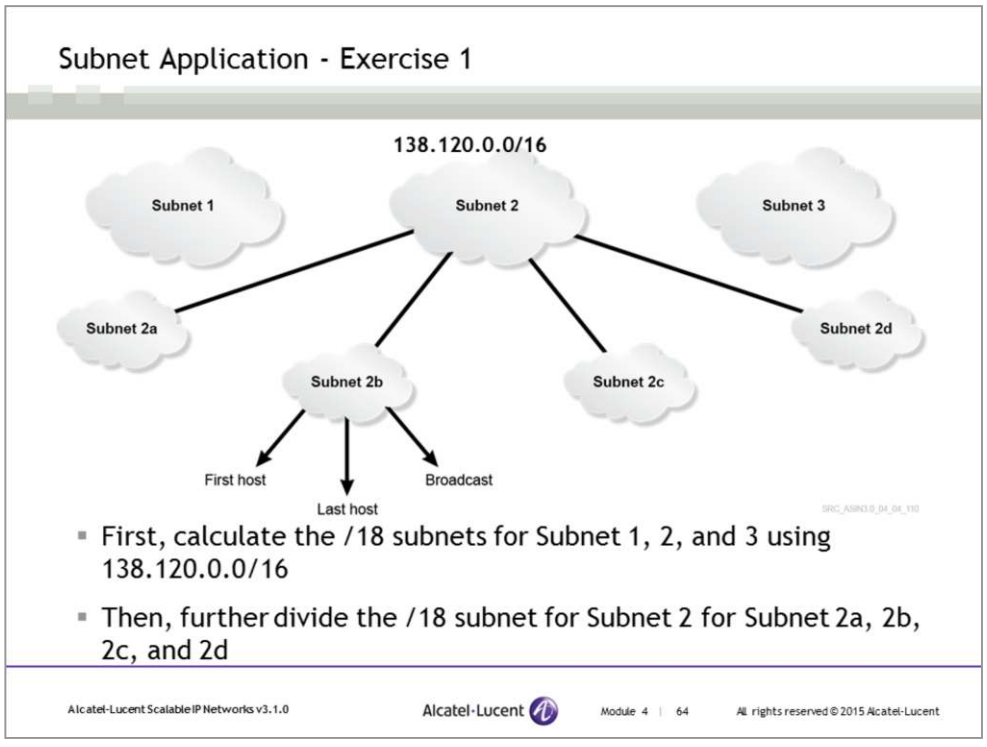
Subnet 3b, 3c, 3d, and 3e: Use 9 bits out of 11 for $2^9 - 2 = 510$ hosts, which is more than the required 400 hosts. The four subnets are assigned with the following network addresses:

172.16.88.0/23, 172.16.90.0/23, 172.16.92.0/23, and 172.16.94.0/23

Note that the sum of all valid hosts is 4094 + 2046 + 510 + 510 + 510 + 510 = 8180. This is because by dividing further, two addresses are reserved for the subnetwork number and broadcast number.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, the administrator is tasked with taking the base network address and subnetting it to support three subnets: Subnet 1, Subnet 2, Subnet 3.

Then, the Subnet 2 address must be further subdivided to support four subnets: Subnet 2a, Subnet 2b, Subnet 2c, Subnet 2d. The administrator must then define the first, last and broadcast addresses for the second sub-subnet.

Subnet 1 network address _____

Subnet 2 network address _____

Subnet 3 network address _____

Subnet 2a network address _____

Subnet 2b network address _____

Subnet 2c network address _____

Subnet 2d network address _____

Subnet 2b

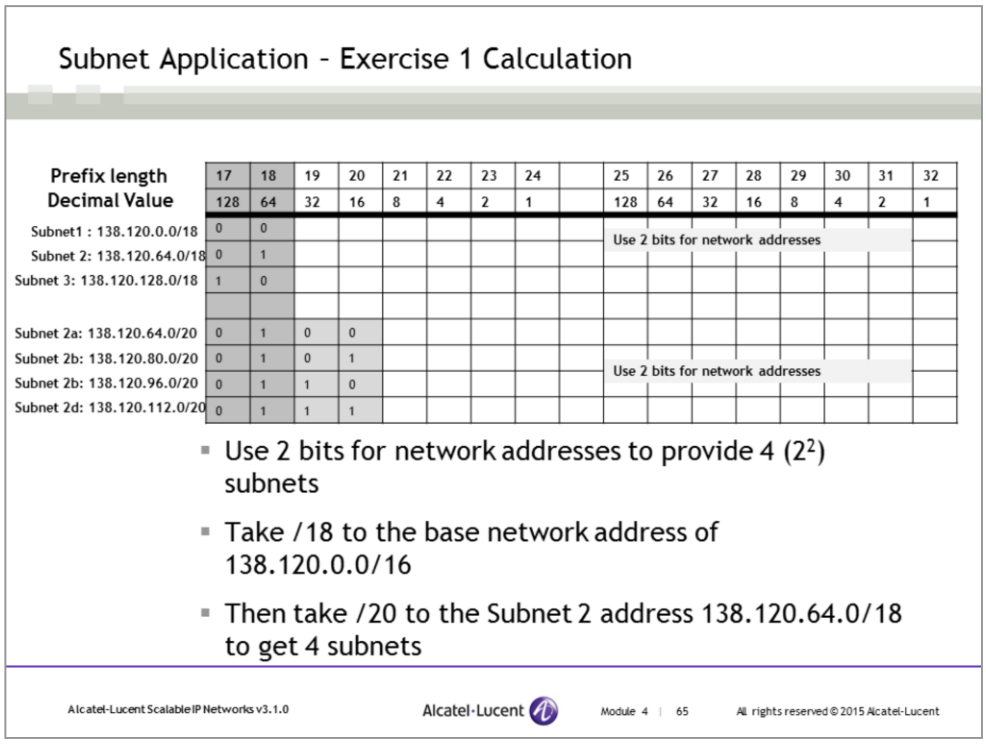
First host address _____

Last host address _____

Broadcast address _____

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The starting address is 138.120.0.0/16. Since you need at least three major subnets (1, 2, 3), you need to borrow 2 bits from the host portion of the address (2^2 = 4 possible subnets). This gives you a mask of /18 and four networks: 138.120.0.0/18 (third octet is binary **00**000000), 138.120.64.0/18 (third octet is binary **01**000000), 138.120.128.0/18 (third octet is binary **10**000000), and 138.120.192.0/18 (third octet is binary **11**000000). This solution uses the first three subnets.

Subnet 1 network address: 138.120.0.0/18

Subnet 2 network address: 138.120.64.0/18

Subnet 3 network address: 138.120.128.0/18

Now, you need to further subdivide the 138.120.64.0/18 network into at least four subnets. Again, this means you need 2 more bits borrowed from the host portion (2^2 = 4 possible subnets), so your mask is now /20 and your subnets are: 138.120.64.0/20 (third octet is binary 01**00**0000), 138.120.80.0/20 (third octet is binary 01**01**0000), 138.120.96.0/20 (third octet is binary 01**10**0000), and 138.120.112.0/20 (third octet is binary 01**11**0000).

Subnet 2a network address: 138.120.64.0/20

Subnet 2b network address: 138.120.80.0/20

Subnet 2c network address: 138.120.96.0/20

Subnet 2d network address: 138.120.112.0/20

Recall that two addresses are reserved. The network address has all zeroes in the host bits, and the broadcast address has all ones in the host bits.

Subnet 2b

First host address: 138.120.80.1

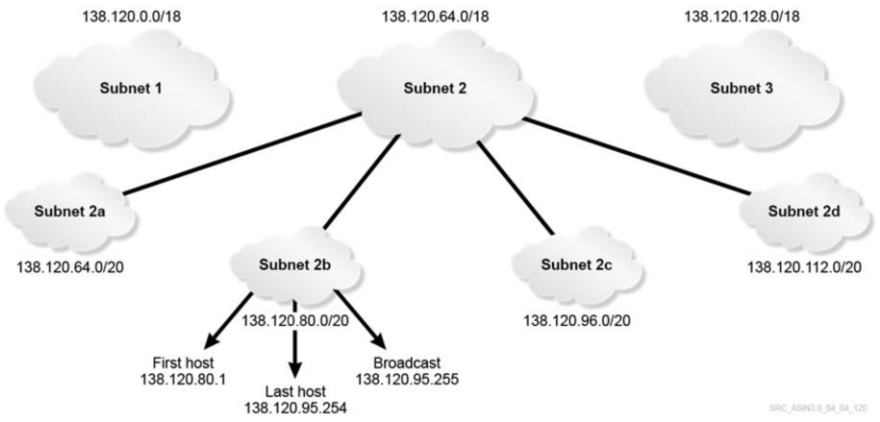
Last host address: 138.120.95.254

Broadcast address: 138.120.95.255

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Subnet Application – Exercise 1 Solution

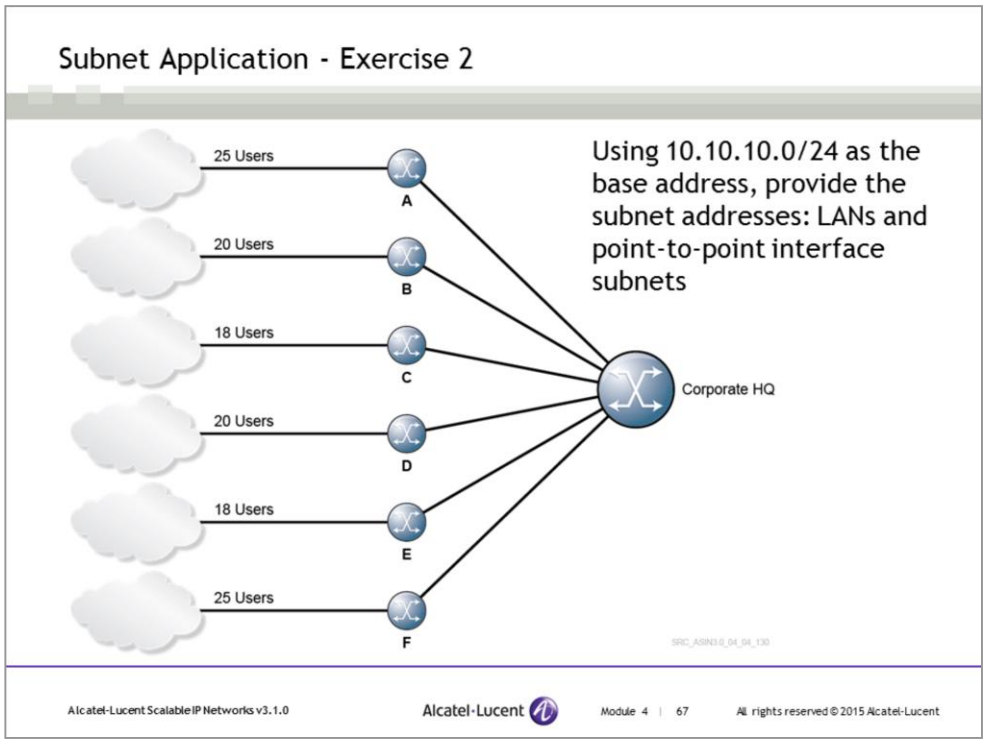


- Your answer may vary since there are multiple solutions that satisfy the requirements

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, the administrator is tasked with taking the base network address and subnetting it to support six subnets, ensuring that each subnet will support its host requirements.

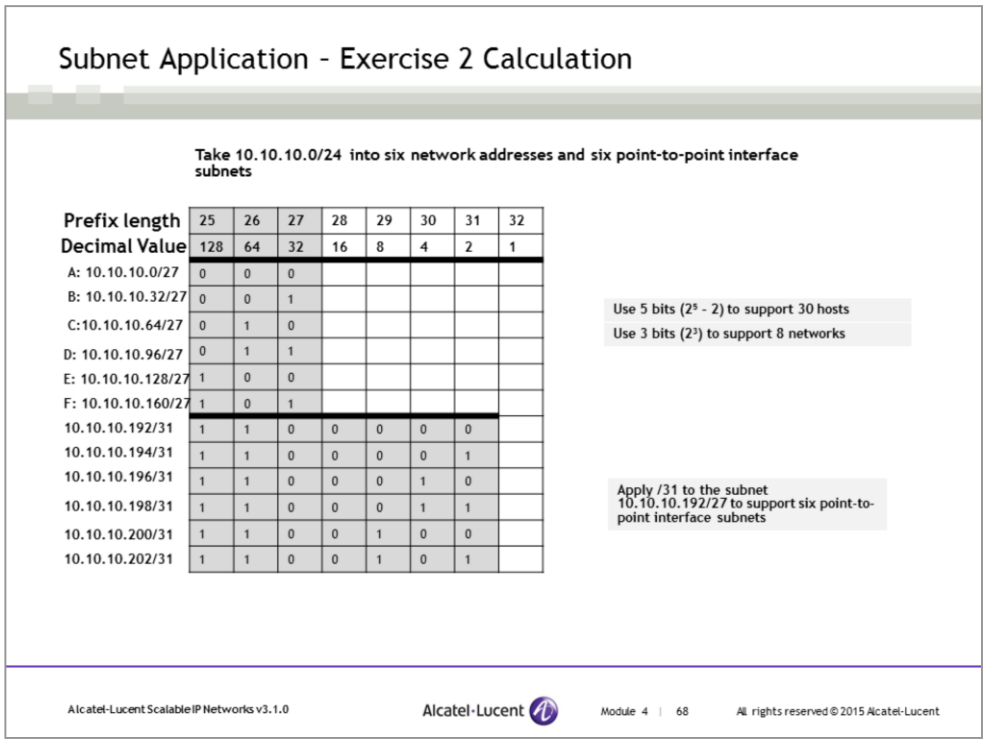
The next task for the administrator is to take one of the subnets and further subdivide it to support the point-to-point links that join the subnet routers to the main router.

Provide a possible address for each of the following:

- Router A LAN _____
- Router B LAN _____
- Router C LAN _____
- Router D LAN _____
- Router E LAN _____
- Router F LAN _____
- HQ - A _____
- HQ - B _____
- HQ - C _____
- HQ - D _____
- HQ - E _____
- HQ - F _____

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The starting address was 10.10.10.0/24. Since six network addresses are needed, 3 bits are borrowed to give a total of 8 subnets (borrowing 2 bits yields only $2^2 = 4$ subnets, borrowing 3 bits gives $2^3 = 8$ subnets). This gives the following subnets: 10.10.10.0/27, 10.10.10.32/27, 10.10.10.64/27, 10.10.10.96/27, 10.10.10.128/27, 10.10.10.160/27, 10.10.10.192/27, and 10.10.10.224/27.

This solution uses the first six subnets for the LANs and the seventh subnet for the point-to-point link between HQ and the routers. Three bits are borrowed from the 8-bit (32-24) host address, which leaves 5 bits for hosts yielding $2^5 = 32$ addresses per subnet, subtracting two addresses for the network address and the broadcast address gives 30 hosts per subnet. None of the subnets requires more than 30 hosts, it does not matter how they are allocated, so just allocate them in order.

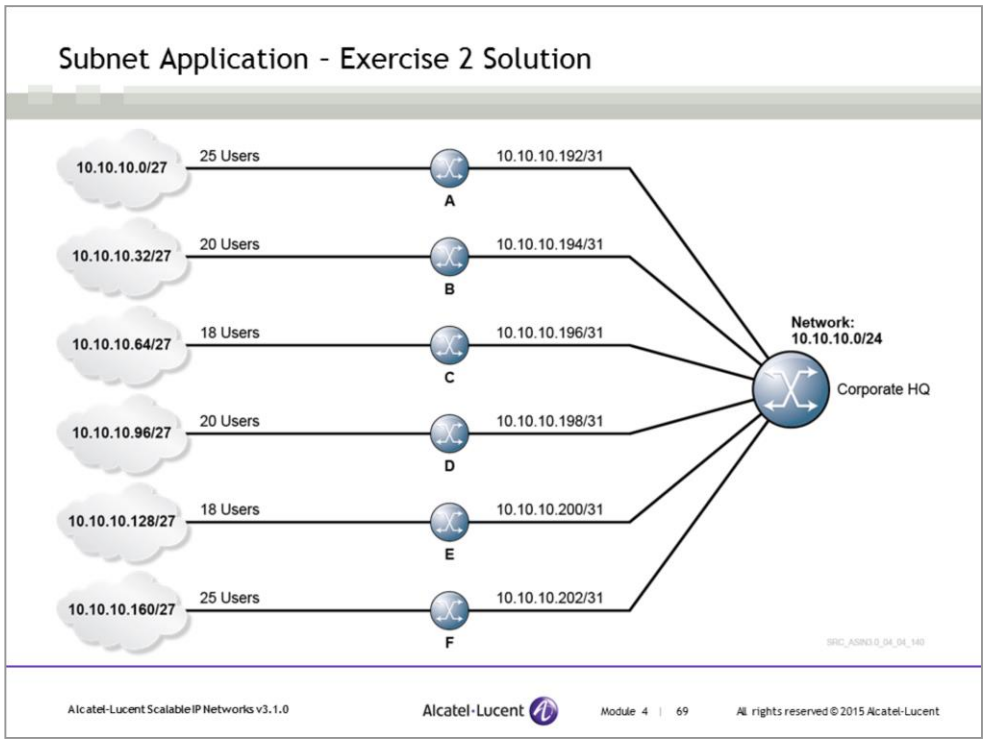
- Router A LAN: 10.10.10.0/27
- Router B LAN: 10.10.10.32/27
- Router C LAN: 10.10.10.64/27
- Router D LAN: 10.10.10.96/27
- Router E LAN: 10.10.10.128/27
- Router F LAN: 10.10.10.160/27

Now choose the next subnet, 10.10.10.192/27, to use for the serial links between the HQ and the routers. Since each point-to-point link only requires two addresses, one for each end, a /31 address can be used.

Apply /31 to the subnet 10.10.10.192/27. This yields the following subnets: 10.10.10.192/31, 10.10.10.194/31, 10.10.10.196/31, 10.10.10.198/31, 10.10.10.200/31, 10.10.10.10.202/31, ..., 10.10.10.254/31. The first six /31 subnets can be assigned to the six point-to-point links between the HQ and routers.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Types of Router Interfaces in 7750 SR

Physical Interface

- Interface that is associated with a physical port
- Almost always assigned with an IP address
- Can be either a point-to-point link or a broadcast link

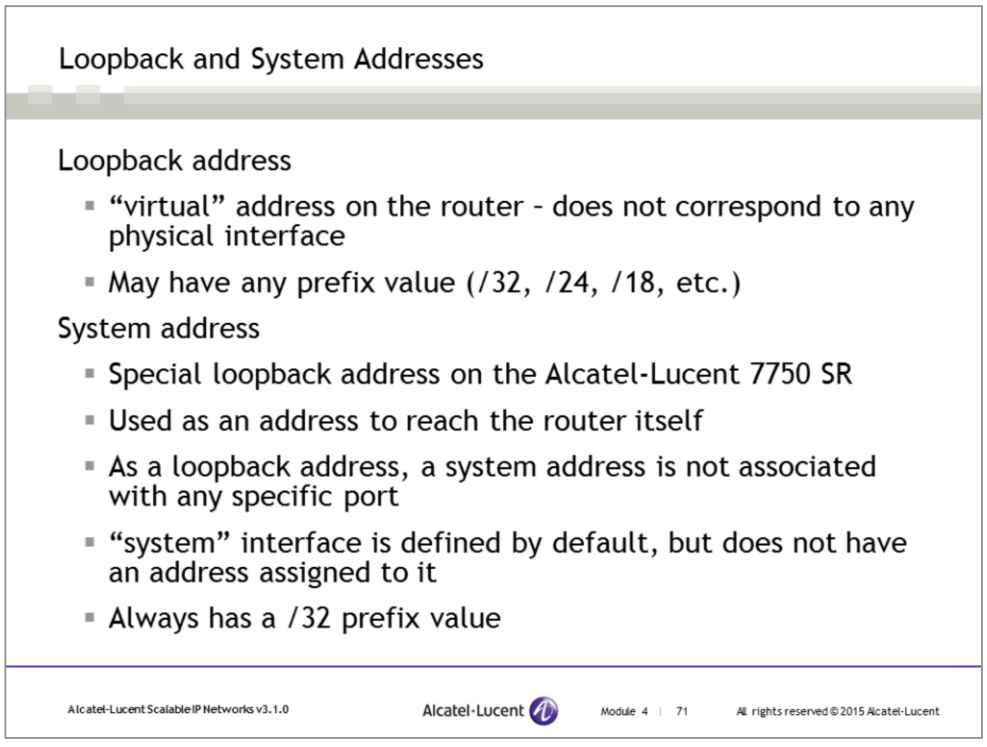
Logical Interface

- Interface that is not associated with a physical port
- Used to reach the router itself
- Loopback interface and system interface are logical interfaces

 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

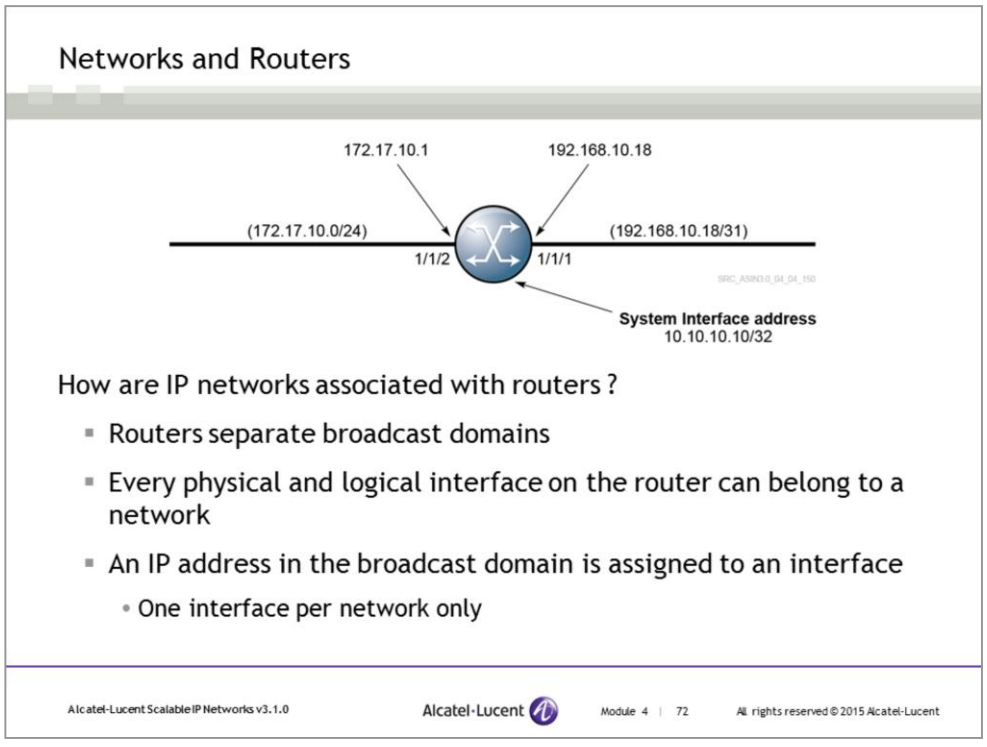


The loopback address (the loopback interface address) is an internal logical address that is not associated with any physical interface. The loopback addresses can have any prefix length.

The system address (the system interface address) is a special loopback address that serves as a router ID for routing protocols such as OSPF and BGP. It is also acts as an address for the router itself. Like any loopback address, the system address can be reached through any active interface on the router. The system address must be a /32 address.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A router interface is a logical entity created to assign local networks in the router. The router interface is commonly referred to as a Layer 3 or (L3) interface. The interface is always assigned an IP address. The IP address is applied along with the subnet mask.

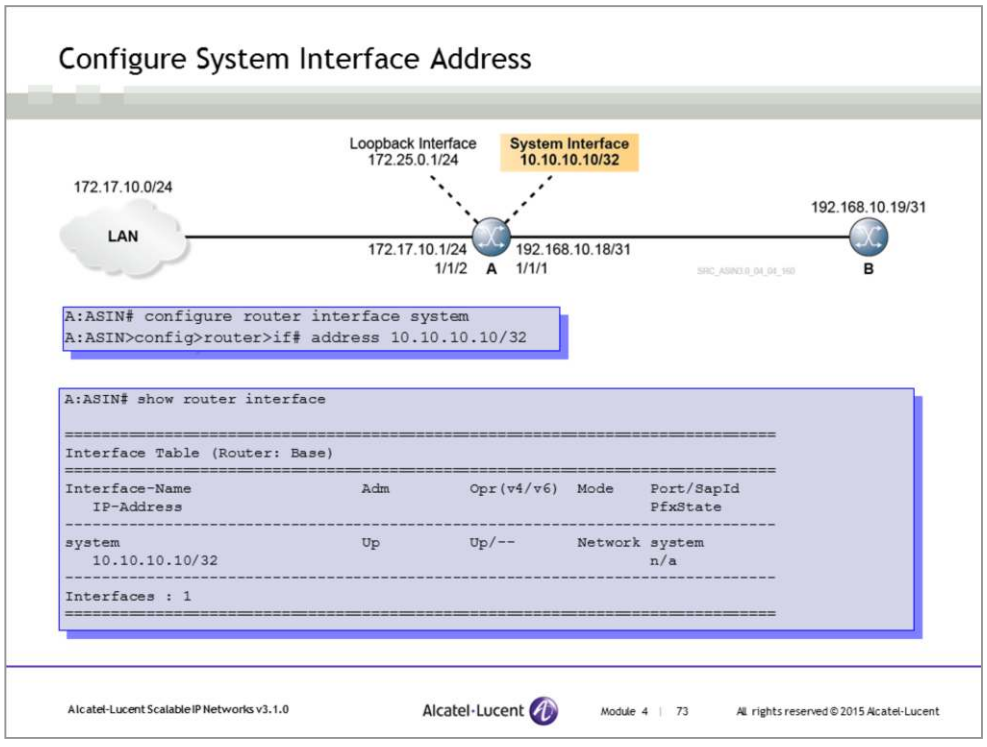
Although the interface is a logical entity, the interface can be associated with a physical port. This is typically done to physically connect the router to another router, switch, hub or host. The other device attached to the router must also be configured with an IP address in the same network as the IP address assigned to the router interface.

An interface that is not associated with a physical port can be associated with a loopback interface and is logical. Remember that a system interface is a special loopback address that serves as a router ID for routing protocols such as OSPF and BGP. The physical and loopback interfaces are considered internal to the router and represent networks within the router.

In this slide, the router has two physical interfaces. An interface with an IP address of 172.17.10.1 belonging to network 172.17.10.0/24 is associated with port 1/1/2. Another interface with IP address 192.168.10.18 belonging to network 192.168.10.18/31 is associated with port 1/1/1. There is also a system interface with an IP address of 10.10.10.10/32.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Router A has two physical interfaces: one is connected to the LAN (Local Area Network) and one is a point-to-point link connecting to Router B.

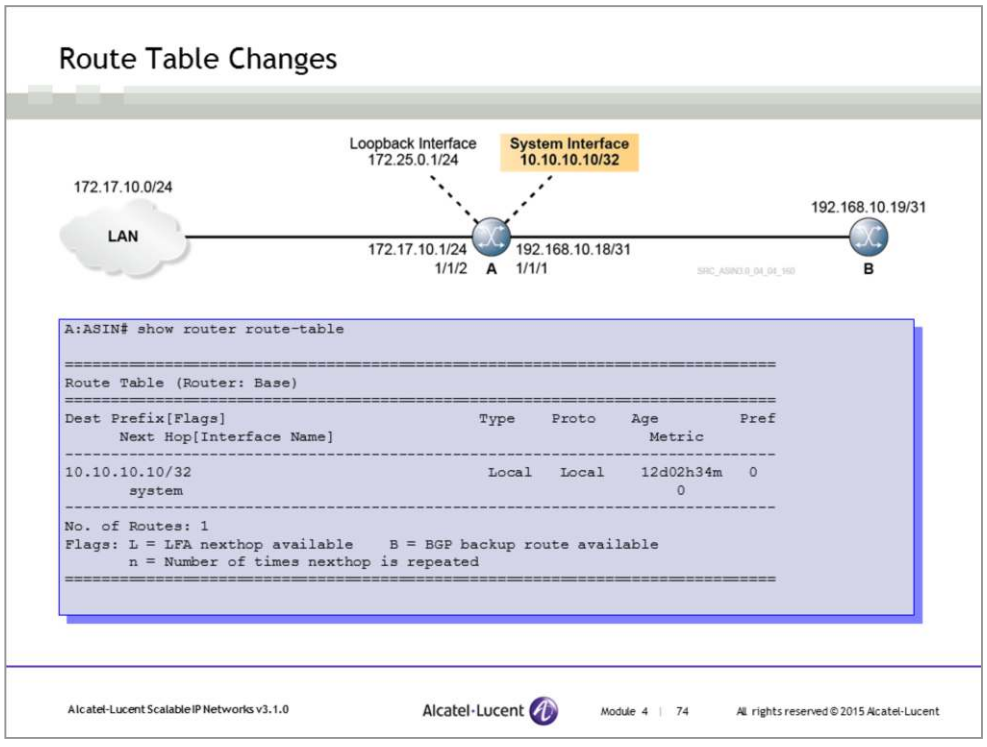
Router A also has two logical interfaces: the system address and the loopback address, both of which are internal to Router A.

This slide shows the steps for a system interface address configuration.

To verify router interface configuration, use the **show router interface** command. The output shows that there is an interface named “system”. The system interface is not associated with an actual physical port.

 All rights reserved © 2015 Alcatel-Lucent

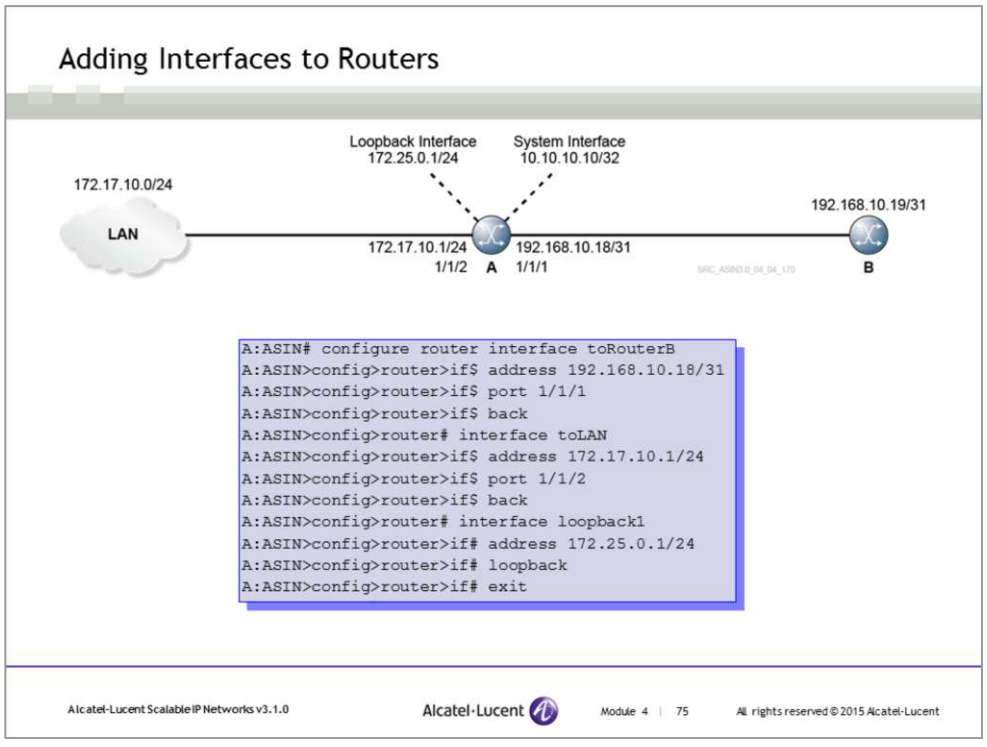
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Once an interface address is configured, a local route is added to the routing table. Note that the local route has the metric value of 0 (lowest cost) and preference value of 0 (most preferred).

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



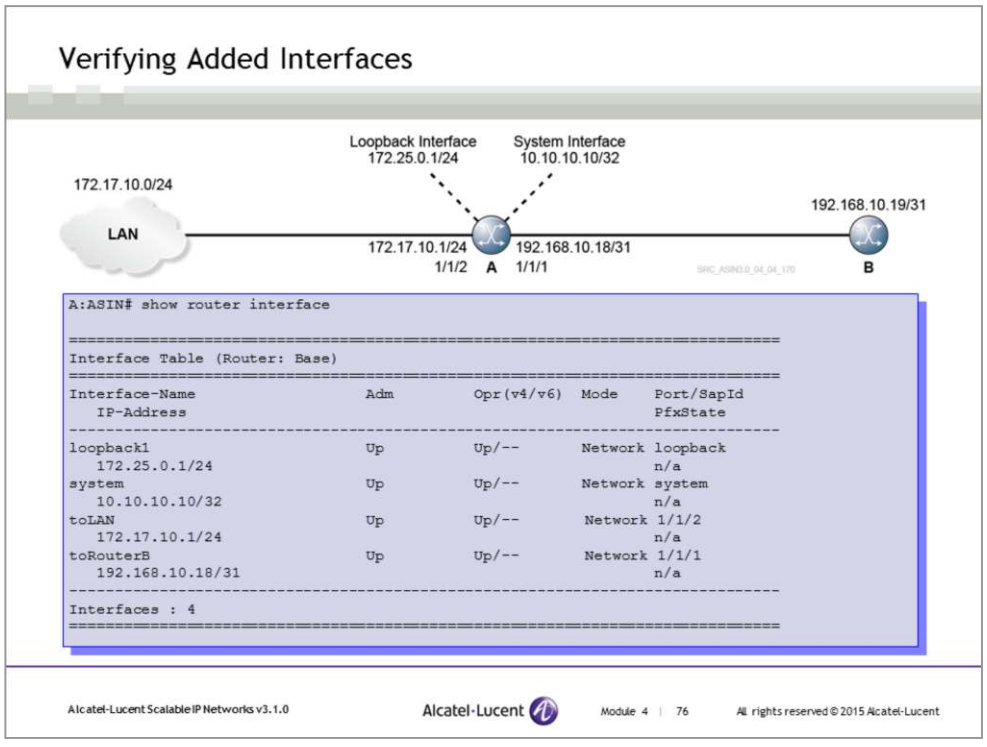
Router A has two physical interfaces: one is connected to the LAN (Local Area Network) and one is a point-to-point link connecting to Router B.

Router A also has two logical interfaces: the system address and the loopback address, both of which are internal to Router A.

In addition to the system interface configuration, other interfaces are configured on Router A as shown in this slide.

All rights reserved © 2015 Alcatel-Lucent

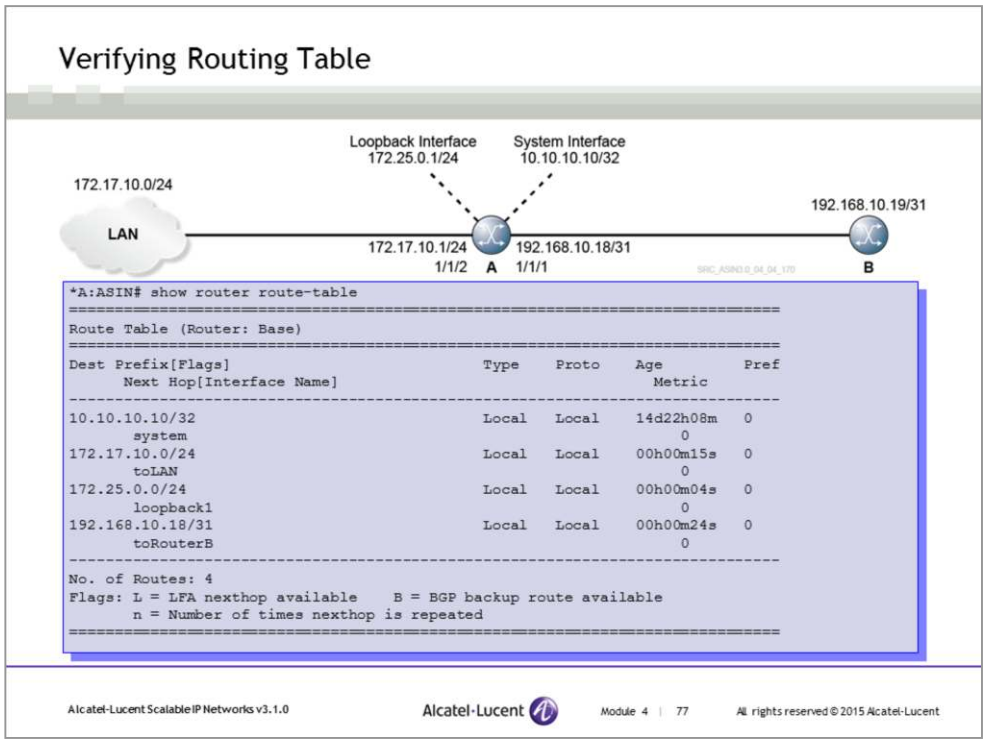
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



To verify router interface configuration, use the **show router interface** command. The output shows that there is one loopback interface named “loopback1” and a system interface. The system interface and the loopback interface are not associated with actual physical ports. There are also two interfaces that are associated with actual physical ports.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

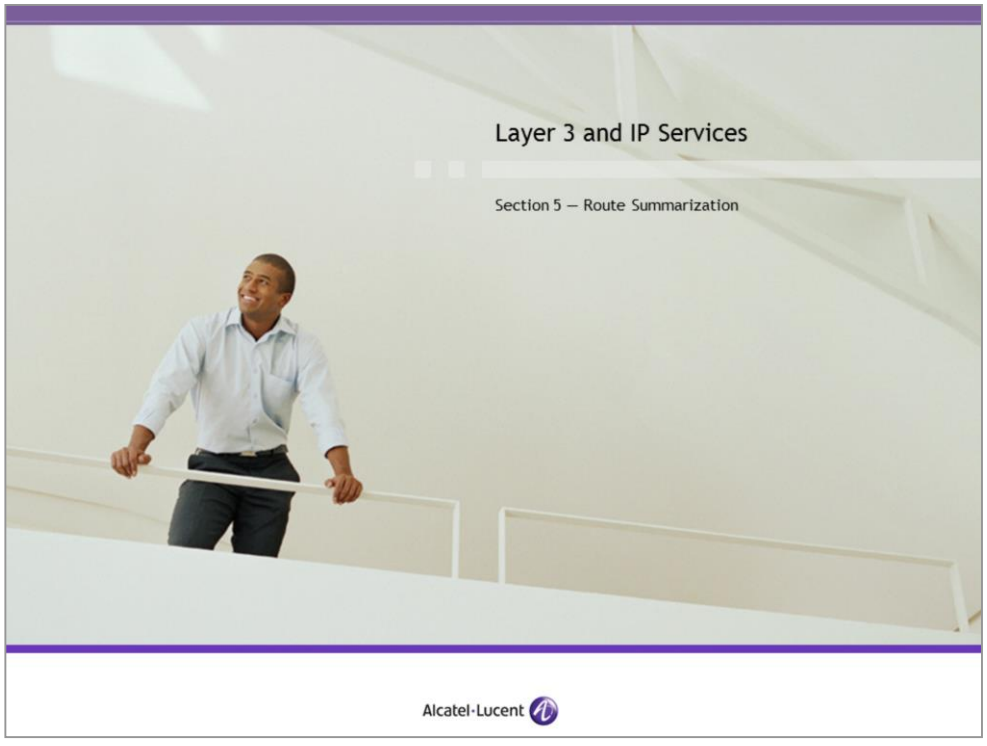


For every interface configured, a local route entry is added to the routing table if the interface is operationally up. Use the show router route-table command to check the content of the routing table. Local routes have the lowest cost (metric value of 0) and are the most preferred (preference value of 0).

Only the network address for the interface is added to the routing table. For example, a loopback interface is configured with an IP address of 172.25.0.1/24. The interface network address of 172.25.0.0/24 is added to the routing table instead of 172.25.0.1/24.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

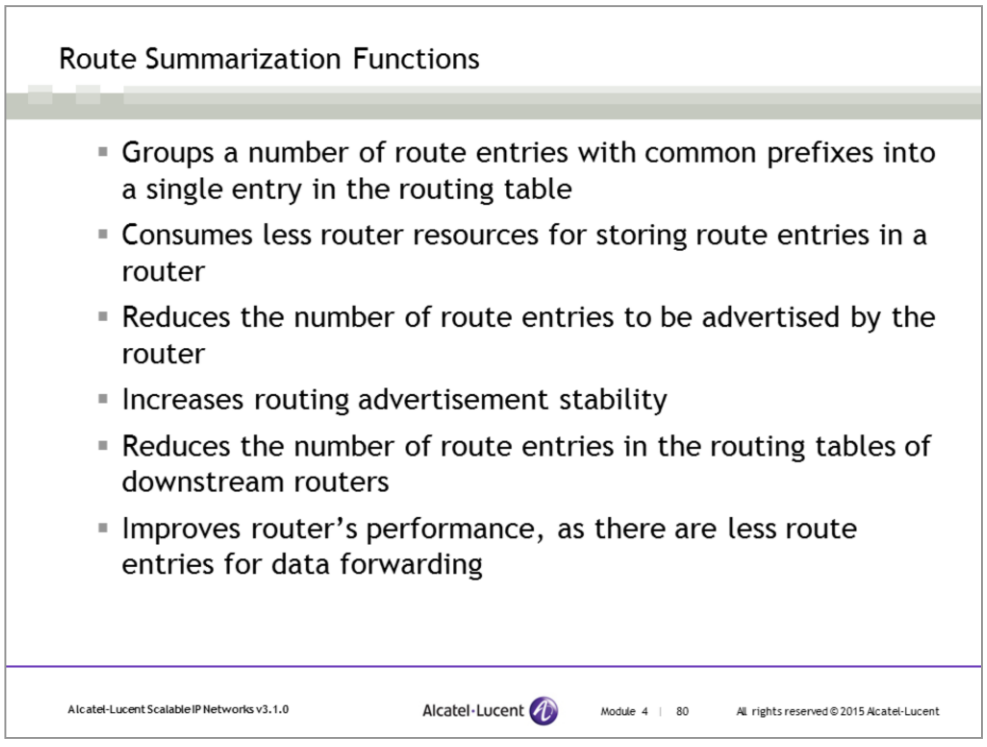
After successful completion of this section, you will be able to:

- Describe the function of route summarization
- Calculate route summarization for a given list of networks

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 4 | 79
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



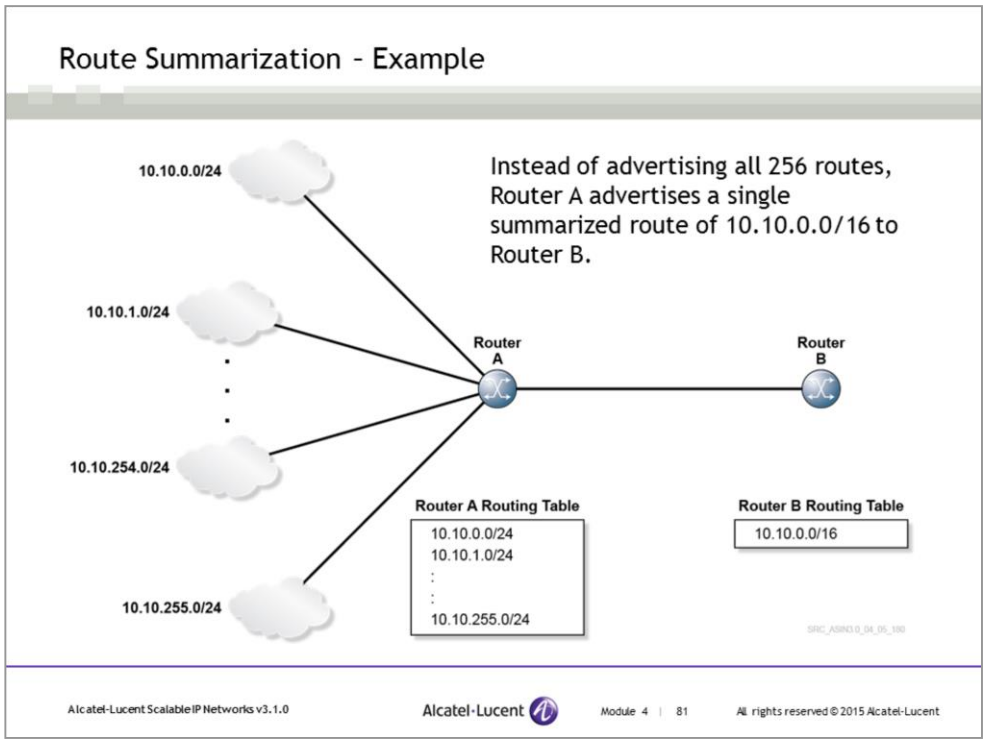
With the rapid expansion of the Internet, IPv4 addresses became exhausted by the 1990s, and the sizes of routing tables expanded exponentially. By eliminating the concept of address classes, Classless Inter Domain Routing (CIDR) allowed for a more efficient allocation of the IP address space. CIDR supports the concept of route summarization, or route aggregation, thus allowing a single route entry to represent multiple networks.

Without route summarization, routers would need a route entry to every subnet in a network.

When address planning is done properly, and when the route summarization is used, all subnets can be represented by as few entries as possible in the routing table. This reduces memory resources required to store route entries in a router. The router advertises fewer route entries to the downstream routers, thereby reducing the number of route entries in the routing table of all downstream routers. Also, if one of the subnets within the summarized route becomes non-operational, the advertising router is not going to withdraw the summarized route because there are operational subnets within the summarized route. As a result, routing advertisement stability is achieved.

 All rights reserved © 2015 Alcatel-Lucent

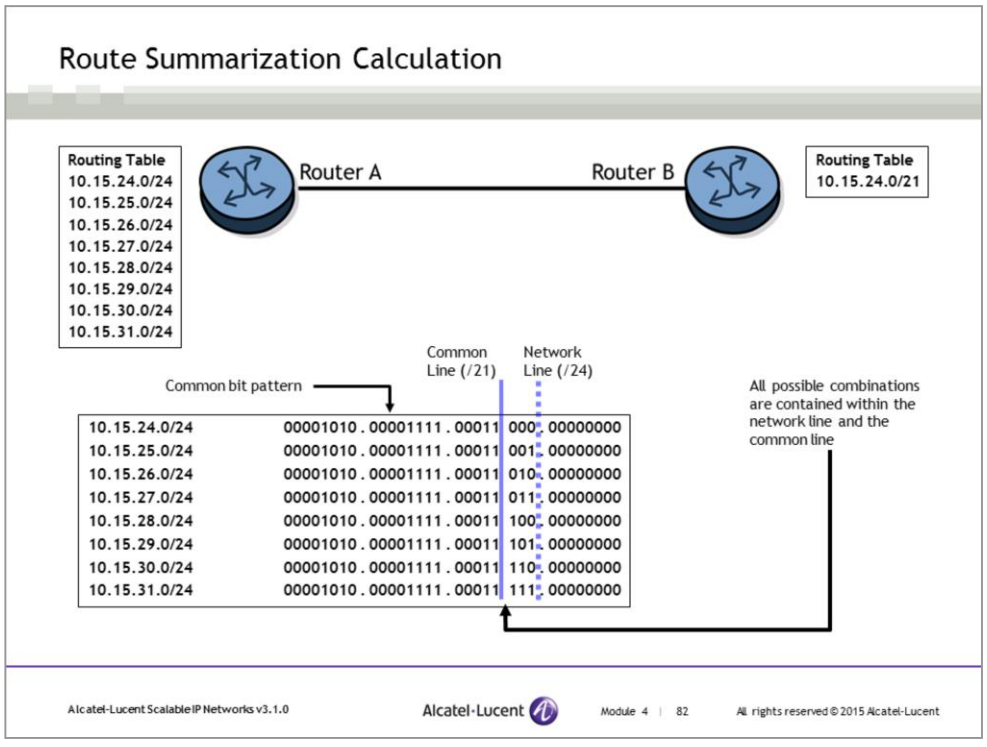
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This is a simple example of route summarization. It is easy to see that Router B only needs one entry of 10.10.0.0/16 to represent all 256 networks on Router A. However, route summarization is not always this simple, and it is important to understand the procedure for calculating a route summarization.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Address planning is extremely important when subnets are first deployed. The subnets should be deployed so that they support the concept of summarization, and so that when summarization is applied, all subnets can be represented by as few entries as possible in the routing table.

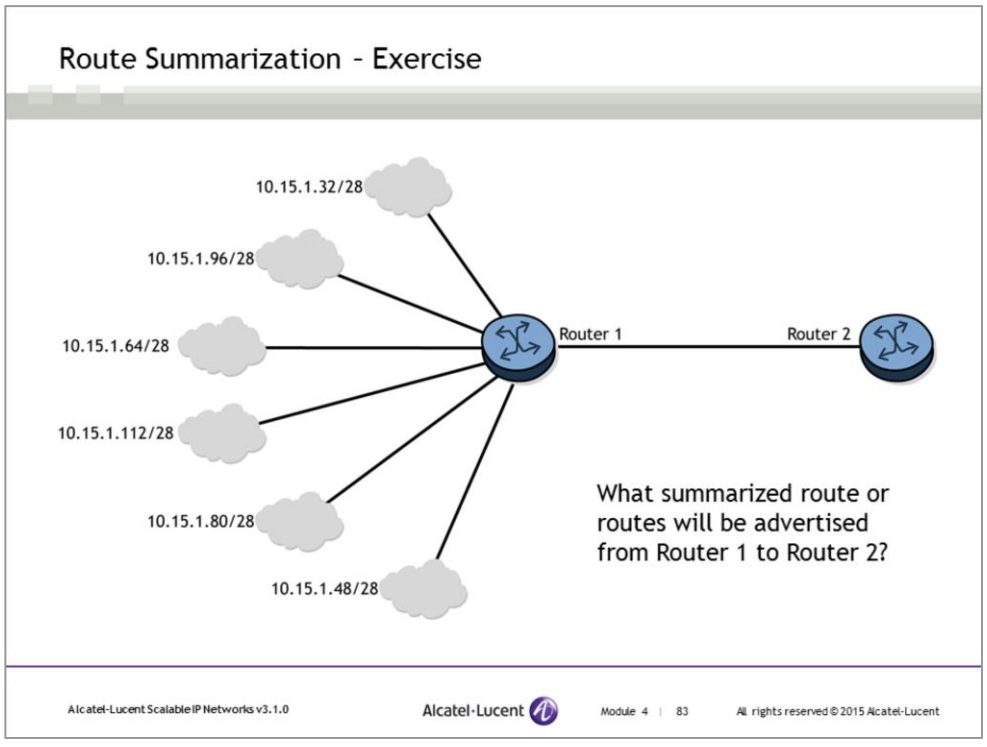
In this slide, Router A supports eight subnets with a /24 prefix. Rather than advertising all eight subnets, the administrator decided to implement route summarization. To see what network address or addresses will be advertised from Router A to Router B, the administrator decided to calculate what the new network prefix(es) should be.

To implement route summarization:

1. Define the octet that will be manipulated by the summarization. In this case, it is the third octet because the first two octets are always 10.15.
2. Identify the original network prefix (/24).
3. Look to the left of the prefix line and identify the area where all of the addresses have the same bit pattern. Draw a line down that portion.
4. Look between these two lines and ensure that all possible bit patterns are contained between the two lines. If this is the case, you can then summarize those bit patterns into (in this slide) a /21 mask.

 All rights reserved © 2015 Alcatel-Lucent

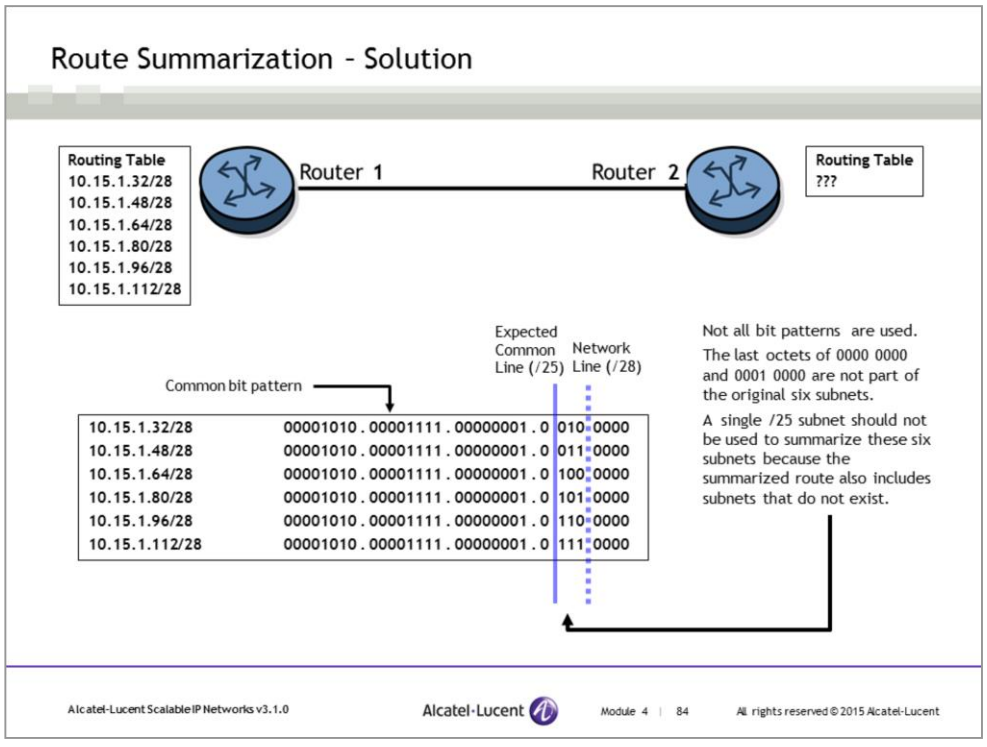
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, the administrator is going to use route summarization on Router 1. What route or routes will be advertised to Router 2?

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



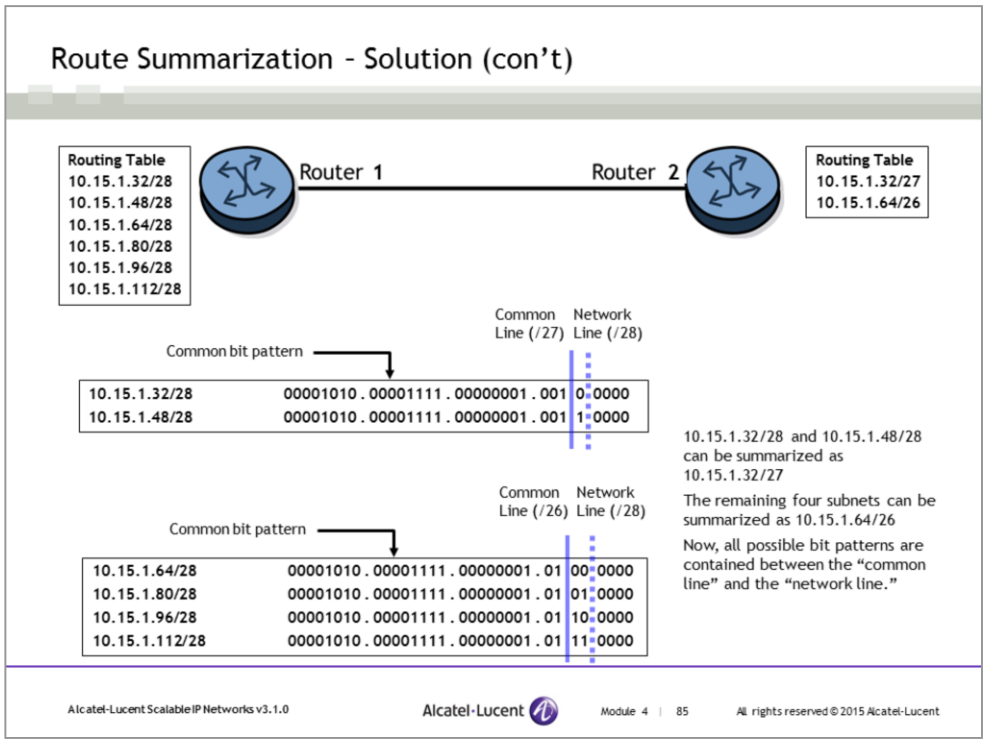
The very first thing to do is to breakdown the subnets into binary. The operations become much easier with the actual bit patterns.

Recall the steps to implement route summarization:

1. Define the octet that will be manipulated by the summarization. In this case, it is the fourth octet because the first two octets are always 10.15.1.
2. Identify the original network prefix (/28).
3. Look to the left of the prefix line and identify the area where all of the addresses have the same bit pattern. Draw a line down that portion. The common line should be /25.
4. Look between these two lines and ensure that all possible bit patterns are contained between the two lines. In this case, not all bits patterns are contained between the two lines. This means that all of these subnets cannot be summarized into a single route advertisement. The last octets of 0000 0000 (0) and 0001 0000 (16) or the subnets of 10.15.1.0/28 and 10.15.1.16/28 are not part of the original six subnets.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



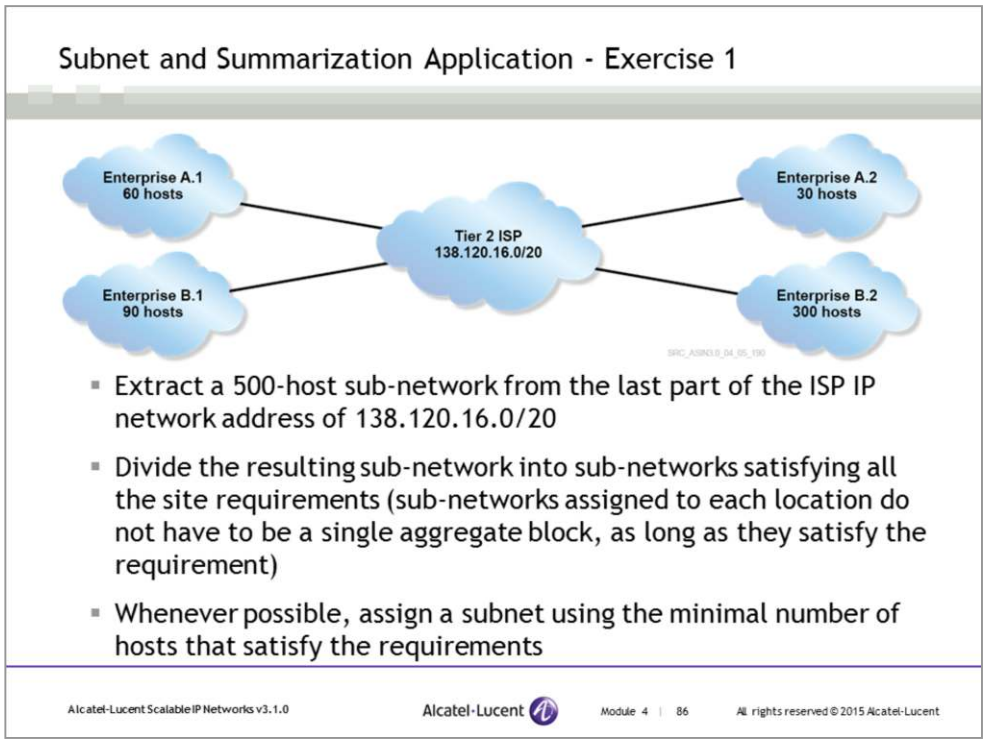
The six subnets cannot be summarized into a single route; they can be summarized into two routes.

10.15.1.32/28 and 10.15.1.48/28 can be summarized as 10.15.1.32/27. All bit patterns are used between /27 and /28.

10.15.1.64/28, 10.15.1.80/28, 10.15.1.96/28, and 10.15.1.112/28 can be summarized as 10.15.1.64/27. Again, all bit patterns are used between /26 and /28.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this exercise, you will design and implement an IP network addressing scheme to support communications between the routers as shown in this slide.

Two enterprises, A and B, are connected to a central Tier 2 ISP. A.1 and A.2 are two of Enterprise A's locations connected to the Tier 2 ISP and B.1 and B.2 are two of Enterprise B's locations connected to the same Tier 2 ISP.

The ISP has a public IP addressing space of 138.120.16.0/20. Enterprises A and B lease their IP addressing from their ISP.

Enterprise A requires an IP addressing scheme that can scale to a maximum of 60 nodes in location A.1 and 30 nodes in location A.2.

Enterprise B requires an IP addressing scheme allowing for a maximum of 90 nodes in location B.1 and no more than 300 nodes in location B.2.

The ISP can only lease 500 IP addresses among the two enterprises and will utilize the last part of its assigned sub-network for both.

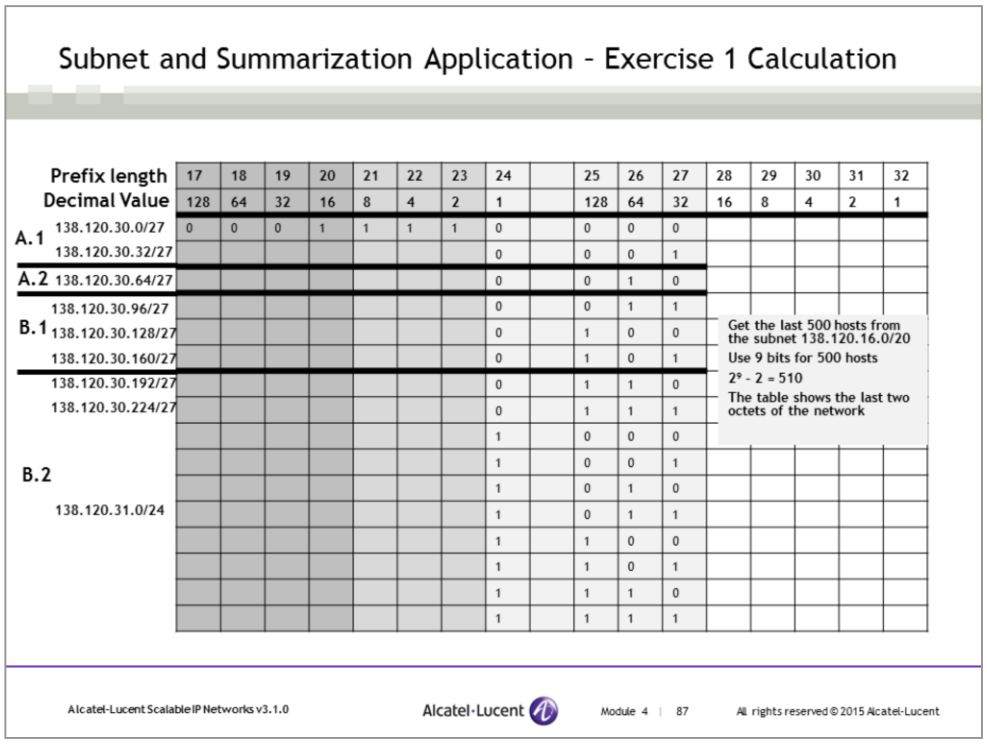
Your tasks are to:

1) Extract a 500-host sub-network from the last part of the ISP IP network address of 138.120.16.0/20.
2) Divide the resulting sub-network into unequal sub-networks satisfying all the site requirements for each of the enterprise locations. Note: The sub-networks assigned to each location do not have to be a single aggregate block as long as they satisfy the number of addresses required.
3) Wherever possible, optimize address space among enterprise locations.

Hint: Divide the assigned ISP IP sub-network into equal blocks satisfying the smallest requirement and then combine the smaller blocks into aggregate or non-aggregate blocks.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Let's extract the last 500 host addresses from the ISP address space 138.120.16.0/20. We know that 9 bits are needed for 2^9 – 2 = 510 host addresses (remember: two addresses are reserved for network address and broadcast address). The last subnet is 138.120.30.0/23 (third octet is binary 0001**111**0).

The smallest subnet requires 5 bits (2^5 – 2 = 30) to support 30 host addresses. Apply /27 to the last subnet 138.120.30.0/23.

A.1 requires 60 hosts; take two 30-host address blocks (/27). This gives a total of 30 + 30 = 60 hosts for Enterprise A.1.

138.120.30.0/27 and 138.120.30.32/27 => can be aggregated into a single address block of 138.120.30.0/26.

A.2 requires 30 hosts; take the next 30-host address blocks (/27). This provides 30 hosts for Enterprise A.2.

138.120.30.64/27

B.1 requires 90 hosts; take three 30-host address blocks (/27). This provides 90 hosts for Enterprise B.1.

138.120.30.96/27,

138.120.30.128/27 and 138.120.30.160/27 => can be aggregated into a single address block of 138.120.30.128/26.

B.2 requires 300 hosts; take ten 30-host address blocks (/27). This provides 300 hosts for Enterprise B.2.

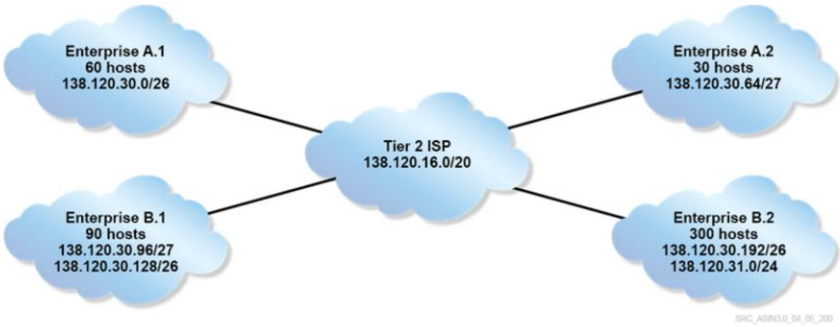
138.120.30.192/27 and 138.120.30.224/27 => can be aggregated into a single address block of 138.120.192/26

138.120.31.0/27, 138.120.31.32/27, 138.120.31.64/27, …, 138.120.31.224/27 => can be aggregated into a single address block of 138.120.31.0/24.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

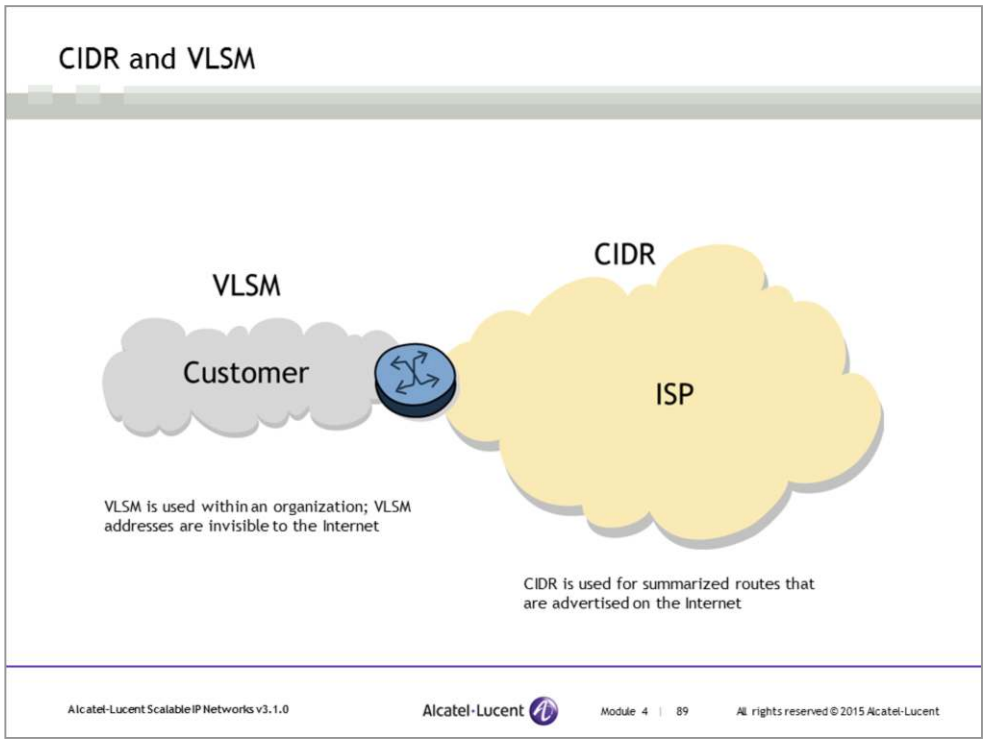
Subnet and Summarization Application – Exercise 1 Solution



 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When you first look at CIDR and VLSM, they seem to provide the same function. Indeed, they are very similar. The difference between the two is how they appear to the Internet.

For both CIDR and VLSM:

- The routing protocol must carry network-prefix information with each advertised route.
- All routers must support the longest-match forwarding algorithm.
- Addresses must be allocated to support route aggregation.

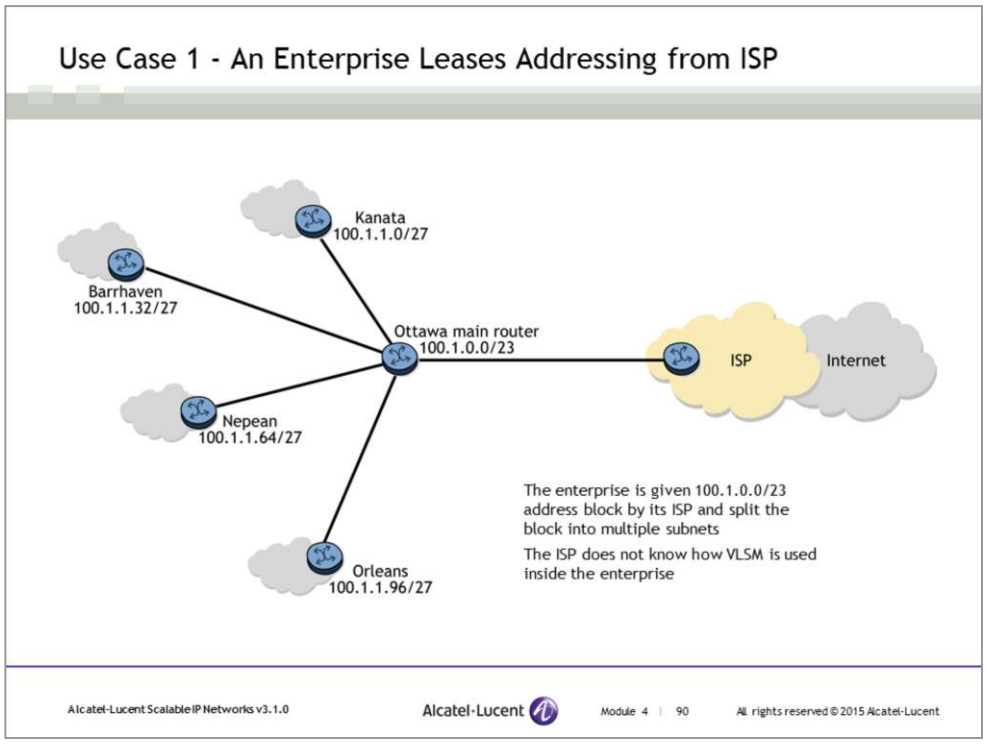
The difference is how the manipulation of the address space appears to the Internet.

VLSM address manipulation is performed on the address that is assigned to an organization and is invisible to the Internet.

CIDR manipulates addresses, and these manipulations are advertised to the Internet.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

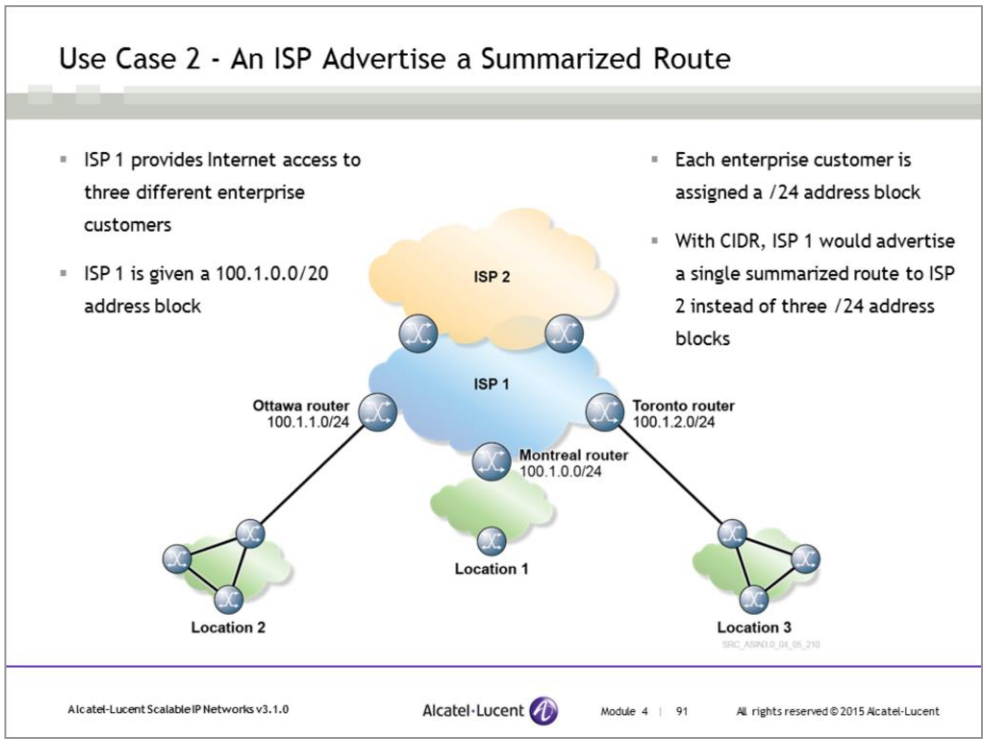


In this slide, an Enterprise in its main location leases its IP addressing from an ISP.

The ISP grants the enterprise ownership to its 100.1.0.0/23 block of addresses and the Enterprise divides its address block into many '/27' subnetwork blocks.

 All rights reserved © 2015 Alcatel-Lucent

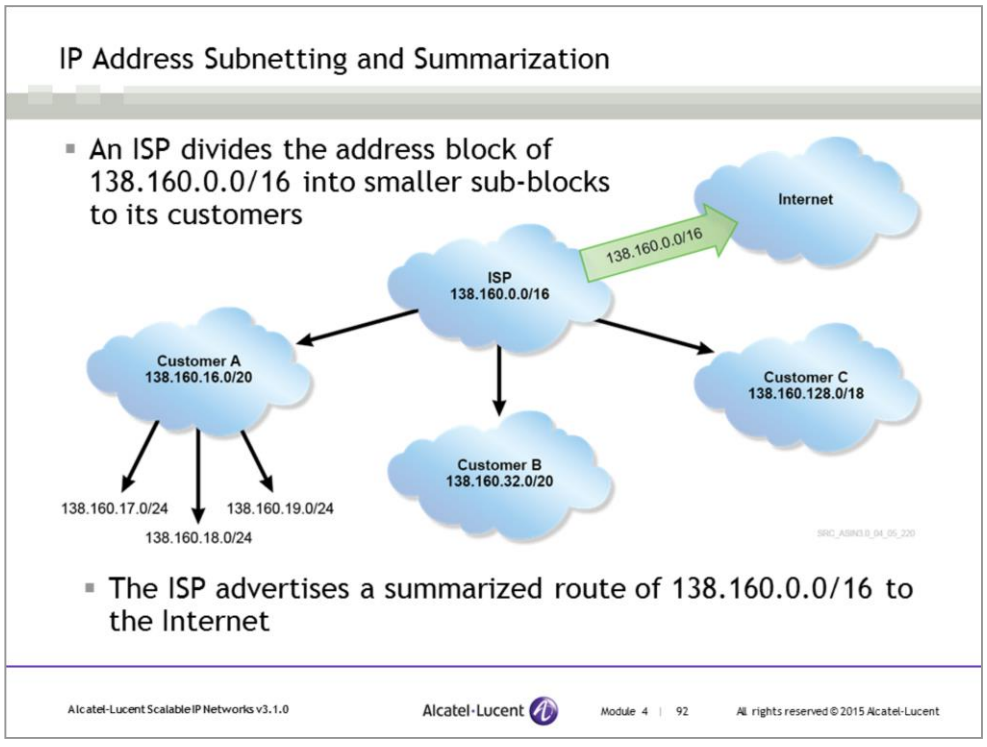
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, ISP 1 provides Internet access to three different enterprises. ISP 1 is given a 100.1.0.0/20 address block; it then divides the block into "/24" address blocks for its customers. If the ISP uses the same "/24" address block for other customers, the ISP can have up to $2^{(24-20)}$=16 customers in total. ISP 1 would advertise a summarized route to ISP 2 instead of the three "/24" address blocks.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IP address subnetting divides an address block into smaller subnets.

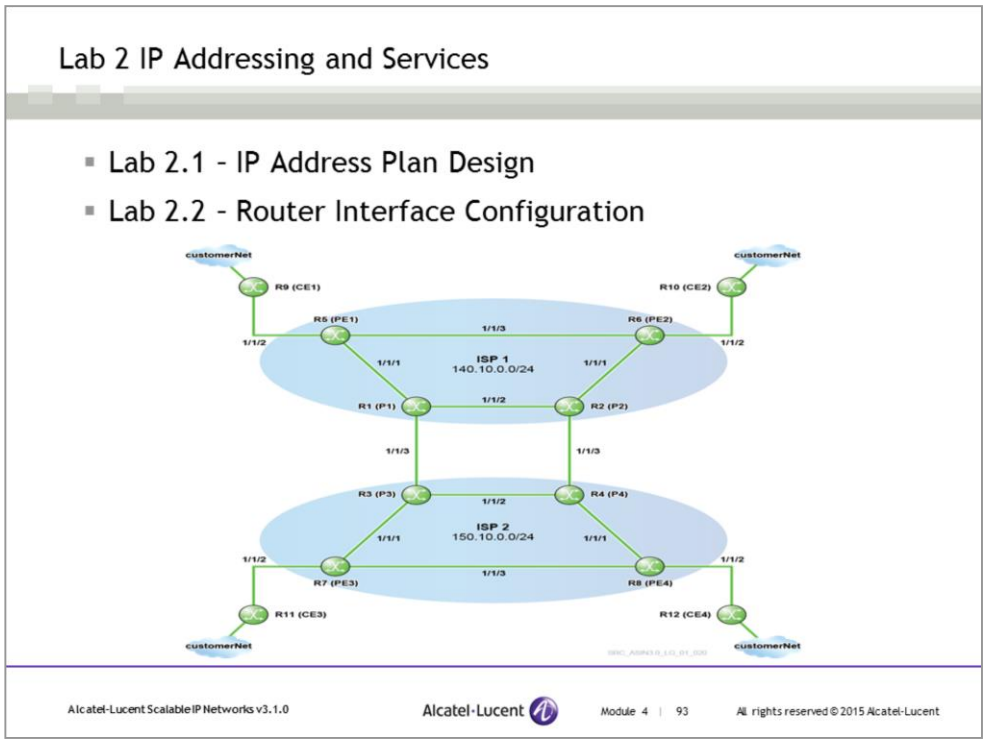
IP address summarization allows a single route entry to represent multiple networks. When summarization or aggregation is applied, all subnets can be represented by as few entries as possible in the routing table.

In this slide, an ISP is allocated with an address block of 138.160.0.0/16 from one of the Regional Internet Registries (RIRs). The ISP then divides its address block into smaller sub-blocks to its customers, A, B and C.

Instead of advertising all subnets to the Internet, the ISP summarizes the subnets as a single summarized route of 138.160.0.0/16 to reduce the Internet's routing table size and increase routing advertisement stability.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

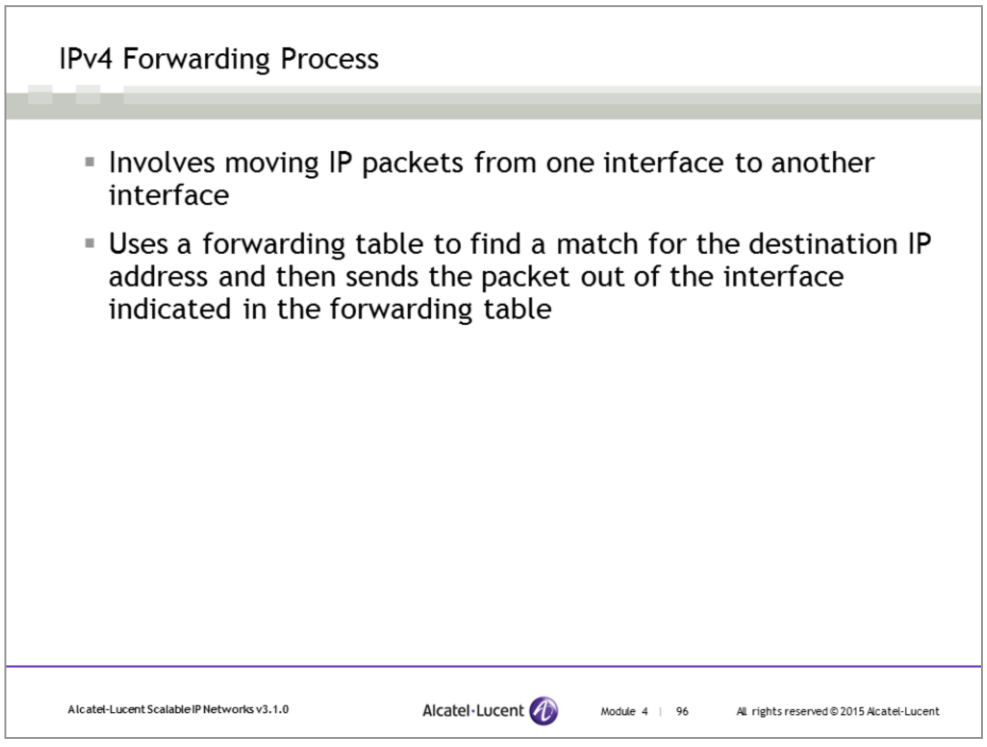
After successful completion of this section, you will be able to:

- Describe how an incoming packet is processed and forwarded
- Use the show command to display the forwarding table

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Forwarding refers to the process of moving transit packets from one interface to another interface. The forwarding process includes accessing the forwarding table to find a match for the destination IP address and then sending the packet out of the interface indicated in the forwarding table.

Forwarding and routing are often used interchangeably; however, there are differences between the two terms.

Forwarding is the process of examining the forwarding table and sending the packet out of the correct destination interface.

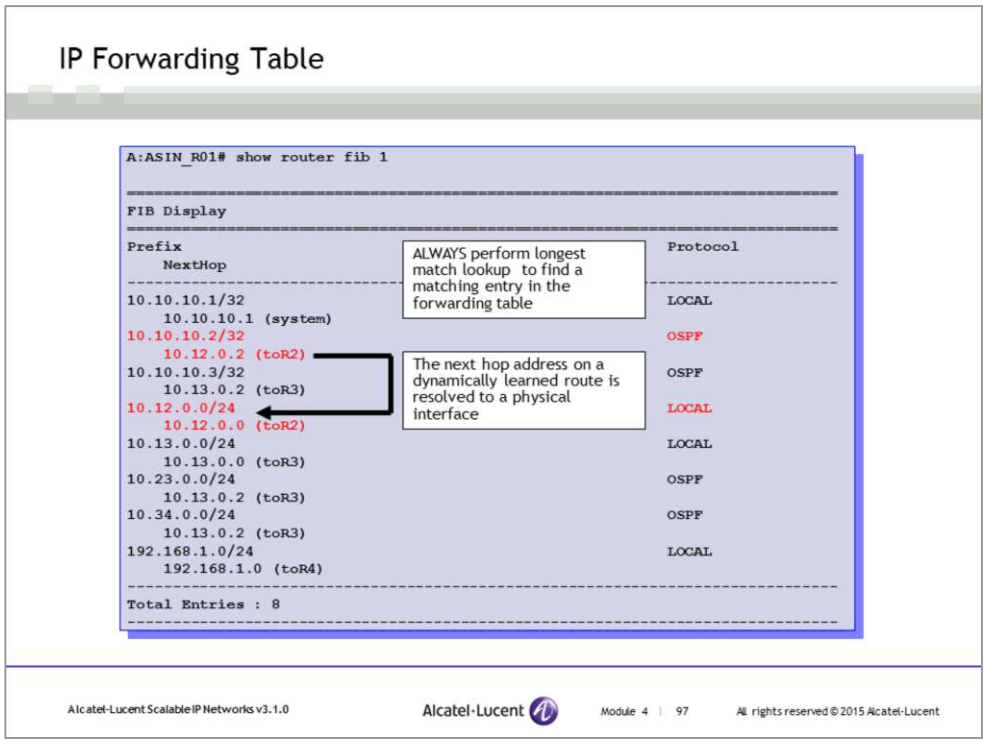
Routing is a more general term and includes not only the forward process described, but the associated processes that a router uses to build the forwarding table as well.

Typically, a routing protocol is used to distribute information throughout a network from one router to another, thus allowing all routers to build up a routing table of destination addresses. Routing protocols will be discussed in Module 5.

This routing table is then used to build the forwarding tables that are used to move packets to the actual router interfaces. On the Alcatel-Lucent 7750 SR, the routing table is maintained by the Control Processor Module (CPM). From the routing table, a forwarding table is constructed and downloaded to each line card. A line card is a physical interface card that resides in a SR chassis.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide gives an idea of what a typical forwarding table looks like. The output of the forwarding table on line card 1 of an Alcatel-Lucent 7750 SR is shown.

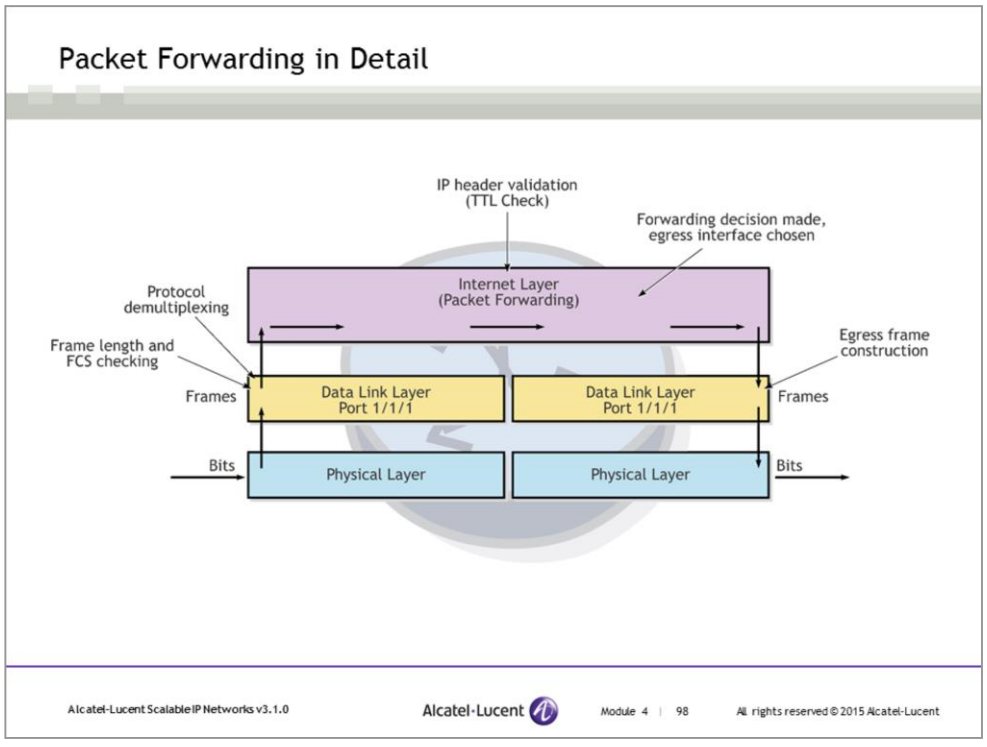
The forwarding table is the information a router uses to move packets from the ingress interface to the egress interface. When a packet comes in the router via a line card, the packet's destination IP address is compared with the content of the forwarding table. If there is a match (longest/most specific match wins) with a prefix in the forwarding table, the packet is switched to the interface as the next hop.

For example, if the incoming packet has a destination IP address of 10.12.0.12, the destination IP address's longest match in the forwarding table is prefix 10.12.0.0/24. Since the next hop interface for that prefix entry is toR2, the packet will be switched to that interface and forwarded on the attached network.

The router has to resolve the next hop address on a dynamically learned route to a physical interface. For example, if the incoming packet has a destination IP address of 10.10.10.2/32, the destination IP address's longest match in the forwarding table is an OSPF route entry 10.10.10.2/32. The next hop address, 10.12.0.2, is then resolved to a physical interface, toR2, using a local route entry. This is how OSPF knows which physical interface it must use to egress the router.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

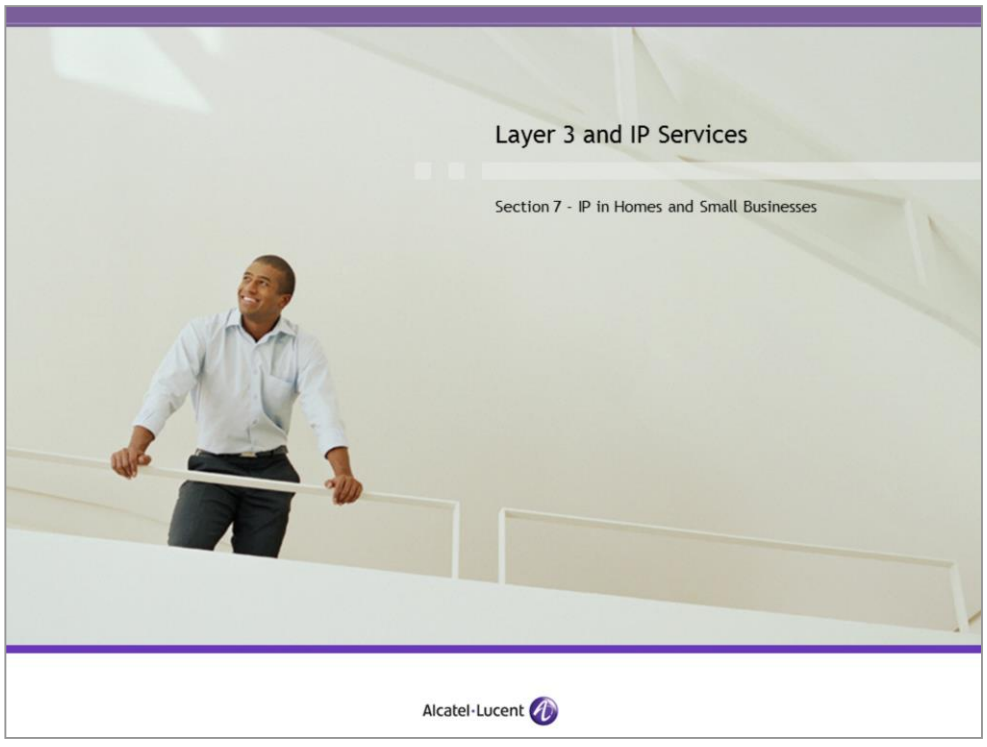


This description of the following process covers some of the key details that are involved in actually moving a packet from one interface to another. The key actions performed by a router are:

1. **Data link layer frame validation**: Basic frame length and FCS verification, as well as the frame sanity checks.
   When a router receives a frame from a LAN, the first step is to read the destination MAC address to ensure that the router is the intended recipient of the frame. The next step, assuming that the router is the intended recipient of the frame, is to check the FCS to see whether there are any errors related to the frame. If there are errors, the router discards the frame at this point.
2. **Network-layer protocol de-multiplexing**: The determination of the upper protocol that needs to receive encapsulated data.
   This step is performed after the L2 information is removed, so that the payload is handed to the correct upper layer.
3. **IP packet validation**: Basic IP header verification.
   A check is performed to determine whether this is an IP packet. The version and ToS fields are examined and removed. The TTL field should be greater than 1; if the TTL = 1, the packet is discarded because this packet's TTL is finished.
4. **Forwarding decision**: Forwarding table lookup.
   Check the forwarding table. If there is a match between the destination IP address in the packet and one of the prefixes (every entry is checked), the egress interface is chosen.
5. **Data link frame construction**: Packet encapsulation.
   The IP packet is now encapsulated in the L2 frame that corresponds to the egress interface. If the interface is Ethernet, new source and destination MAC addresses are added, including the type field, and a new FCS is generated. The packet is sent to the physical layer for transport.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

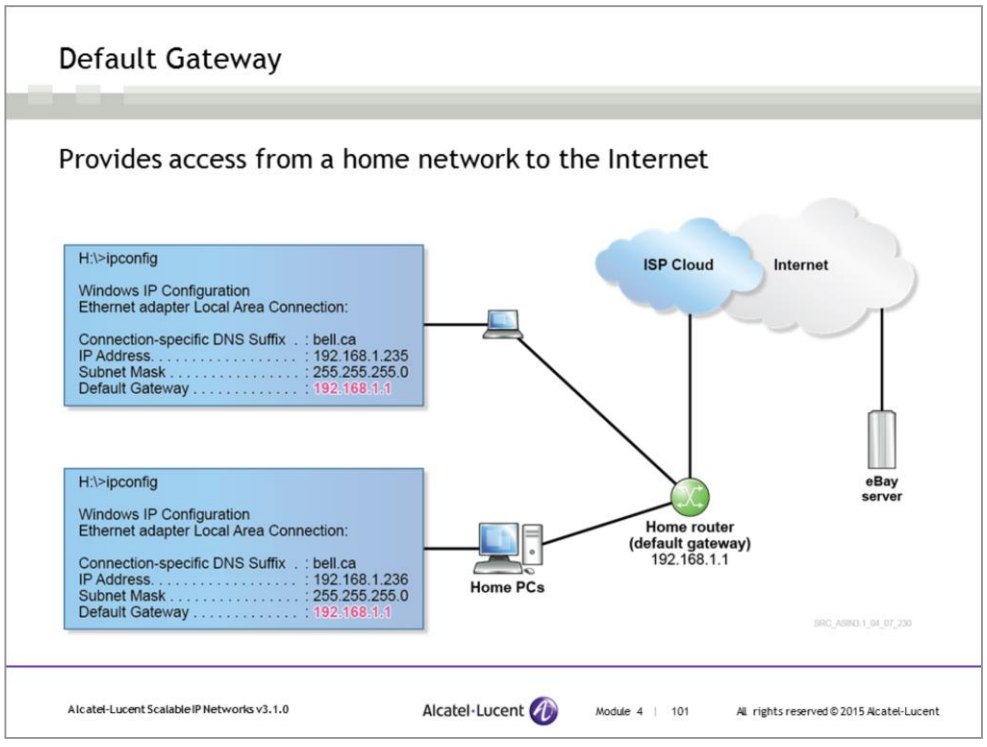
After successful completion of this section, you will be able to:

- Describe a typical IP configuration in a home/business network
- Describe the functions of Network Address Translation (NAT) and Port Address Translation (PAT)
- Describe the operations of DHCP

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 4 | 100 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows a very simple home network.

There are two PCs that are connected to a personal router. The router is then connected to the ISP. The demarcation point is the home router.

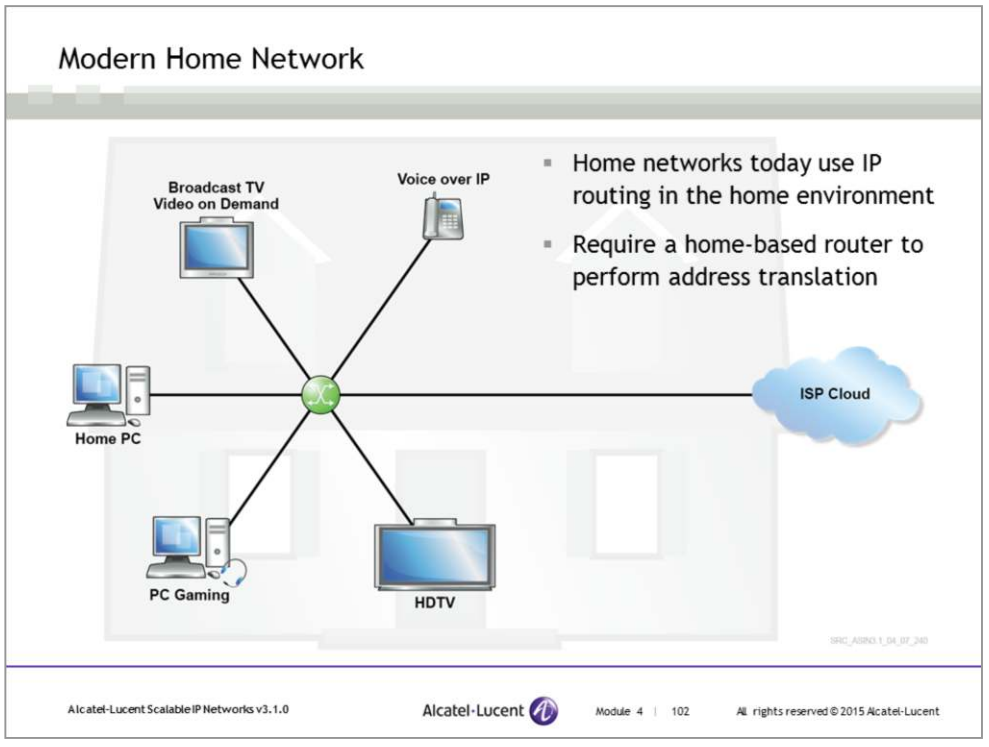
In order to communicate to the Internet, each of the PCs needs a unique routable IP address (typically a private IP address). For traffic from the PCs to the Internet, a designated router address is provided, which is the default gateway. The IP address is the address of the interface on the home router that faces the home network.

Since the personal PCs are on the same network, they can communicate with each other without accessing the Internet.

For a personal PC to access the eBay site, the IP packet composed will contain the source address of the PC, and the destination address of eBay. The PC does not know where the server for eBay exists and the packet is directed to the default gateway, which knows where to forward the packet.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Modern home networks, such as the one shown in this slide, support multiple services. These services can be delivered using one technology by a one provider or by multiple service providers. A personal router is managed at the home and not at the location of the service provider. On one end, the router connects to the home network; on the other side, it connects to the service provider's access device.

All the services (in this single provider/multiple services scenario) are sent to the service provider.

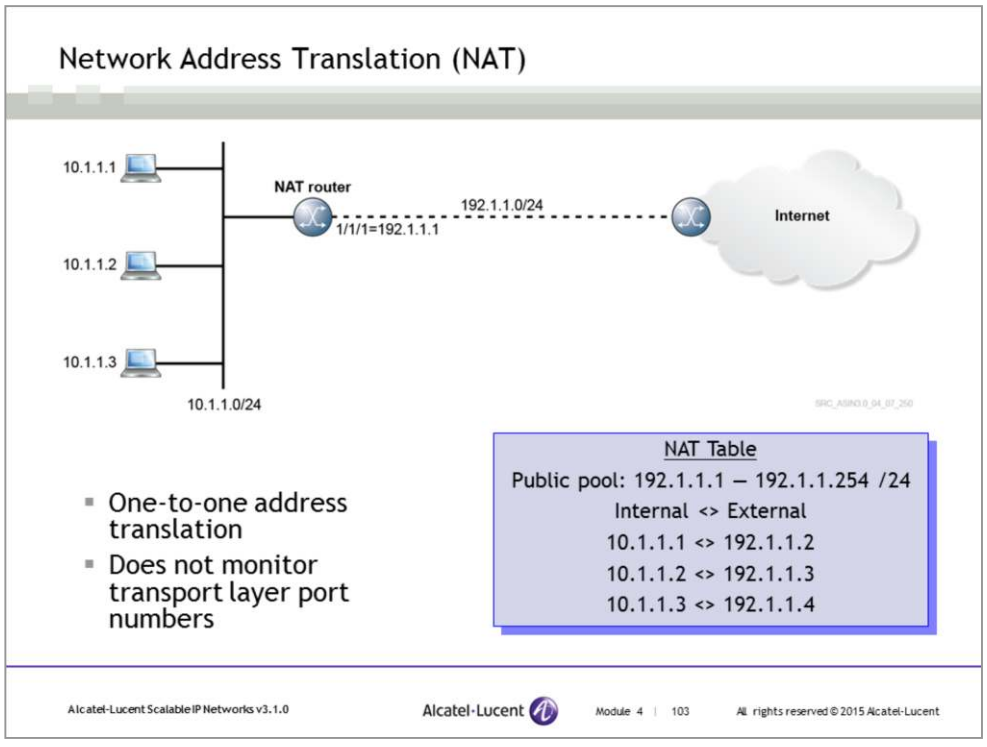
Every device in the home in this scenario requires an IP address to connect to the Internet. There are several disadvantages:

- It is not financially viable to have unique public IP routed addresses. Also, this is not scalable.
- For the traffic to be received by each device, the ISP needs to monitor every home device for a single access point. The ISP is typically not interested in maintaining multiple IP addresses for the average home user.

The best scalable solution for now is a home-managed router, which assigns private IP addresses to each of the home devices and has a public IP address that represents the home to the ISP. Recall that private IP addresses are addresses that can be used by anyone for their own private networks, but are not routable on the Internet. This is an ideal solution for a large number of devices that need to communicate with each other using private addresses. They can all use a single public address to communicate with devices on the Internet. This is possible by using Network Address Translation (NAT) or Port Address Translation (PAT).

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



NAT is defined in RFCs 2663 and 3022. The RFCs refer this type of NAT as “Basic NAT”.

NAT and PAT were created to alleviate the stresses of IP address allocation. Working closely with the private IP address ranges, NAT and PAT allow for private IP addresses to be translated into public IP addresses. This translation can be in one of two forms.

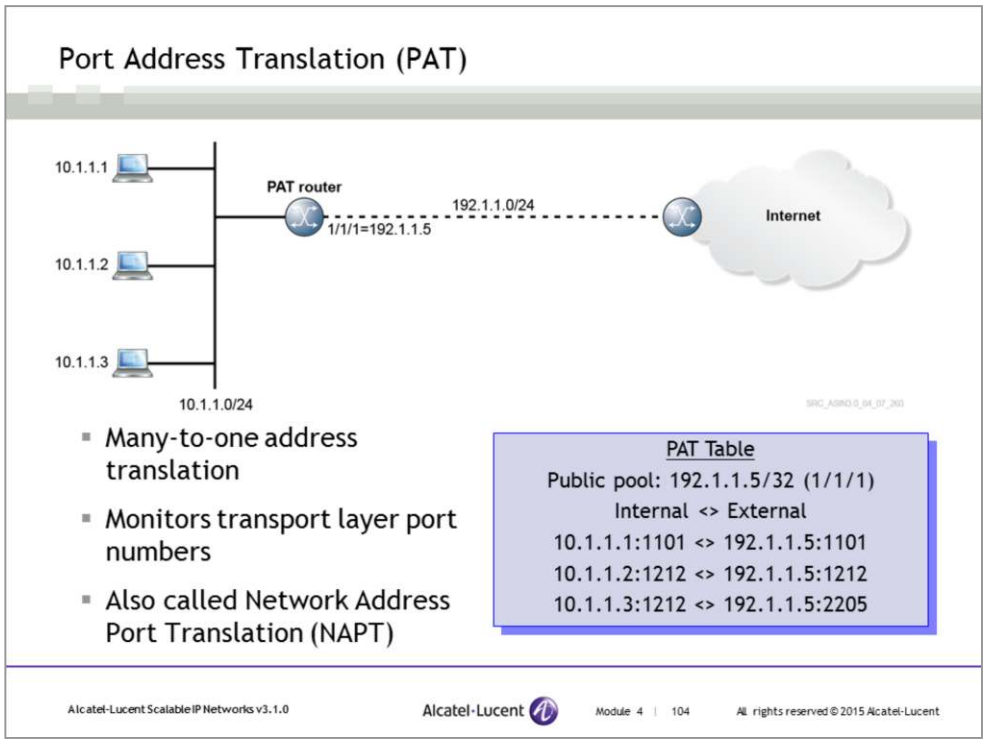
The first form of translation is “one-to-one” translation, also known as NAT. One private IP address is translated to one public IP address. In this form, the transport-layer (TCP or UDP) port numbers are not monitored or modified. This allows all applications to function normally without any change to the upper layers. The disadvantage of this form of translation is that there must be a pool of available IP addresses to support all the private IP-addressed clients. If all of the IP addresses in the pool are in use and there is a new NAT requirement, a failure will occur because there is no available IP address in the pool of public IP addresses.

In this example of NAT, the range of public IP addresses is from 192.1.1.2 to 192.1.1.254. Each client that sends traffic through the router is mapped to one IP address in the pool. If 253 clients are actively sending traffic through the router and if the 254th client tries to send traffic out the router, the traffic cannot be sent because there are no available public IP addresses to use for NAT. Although this limits the number of clients that can simultaneously use this NAT router, it does not limit the types of applications that each client can use.

Note that the Alcatel-Lucent 7750 SR can support Network address translation (NAT) or Port address translation (PAT) using Multiservice Integrated Adapter (MS-ISA). MS-ISA was described in Module 2.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The second form of translation is “many-to-one”, also known as port address translation (PAT). RFCs 2663 and 3022 refer this type of NAT as network address port translation (NAPT).

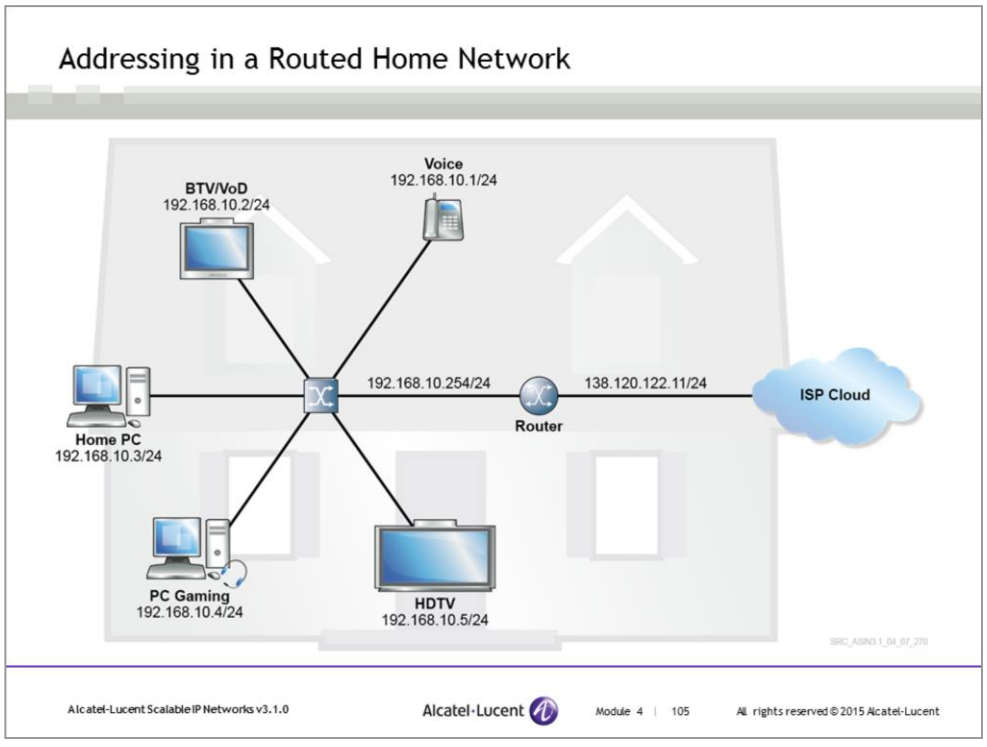
One public IP address supports multiple private IP addresses simultaneously. To accomplish this, the router must not only map the IP address of the client device, but must also map the port number in use by the client. As translation occurs, the IP address is changed to one public IP address. To keep track of the multiple streams of traffic from client devices, the port numbers are mapped to unique port numbers in the database. This port change is transparent to the client.

This slide shows a PAT router keeping track of source port numbers in the database. PAT maintains a list of upper-layer ports and will alter the source port numbers if there is a duplication.

Most modern applications do not have a problem with the change of port. However, some applications (mostly legacy applications) require specific source and destination port numbers. If the router modifies the source port to a port that differs from the port that the application expects or requires, the application may not function correctly. This is rarely a problem with more recently developed applications.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows a typical home network where all of the home devices have their own private IP addresses in the 192.168.10.0/24 range. The router will use a PAT table to keep track of each address and port translation that occurs.

The router interface that faces the ISP, which is sometimes referred to as the Wide Area Network (WAN) side, has a public IP address of 138.120.122.11/24.

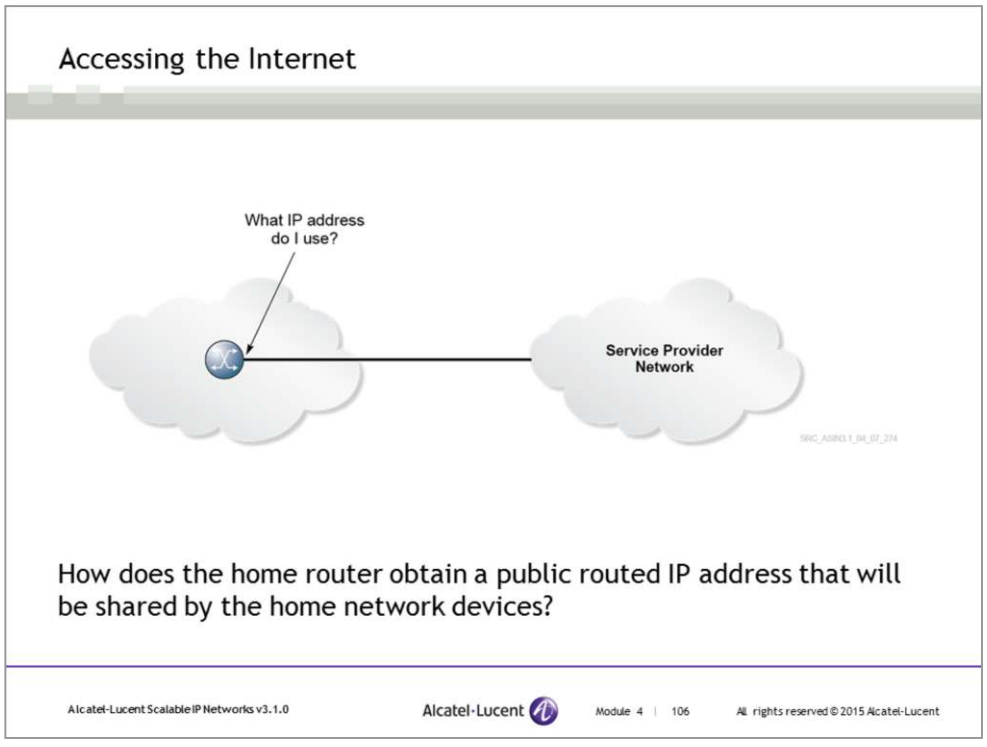
The router interface that faces the home network is based on the private address range 192.168.10.0/24, and each device, including the router interface, has an IP address from that subnet.

The default gateway programmed into every IP device for Internet access is the router interface address that faces the home network, which in this case is 192.168.10.254/24.

When any device attempts a TCP/UDP connection to the Internet, the home router handles the address translation by using a port address translation table.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Every home router and PC that needs to connect to the Internet requires a public IP address. These IP addresses must be requested from the Internet Assigned Number Authority (IANA) and its regional subsidiaries.

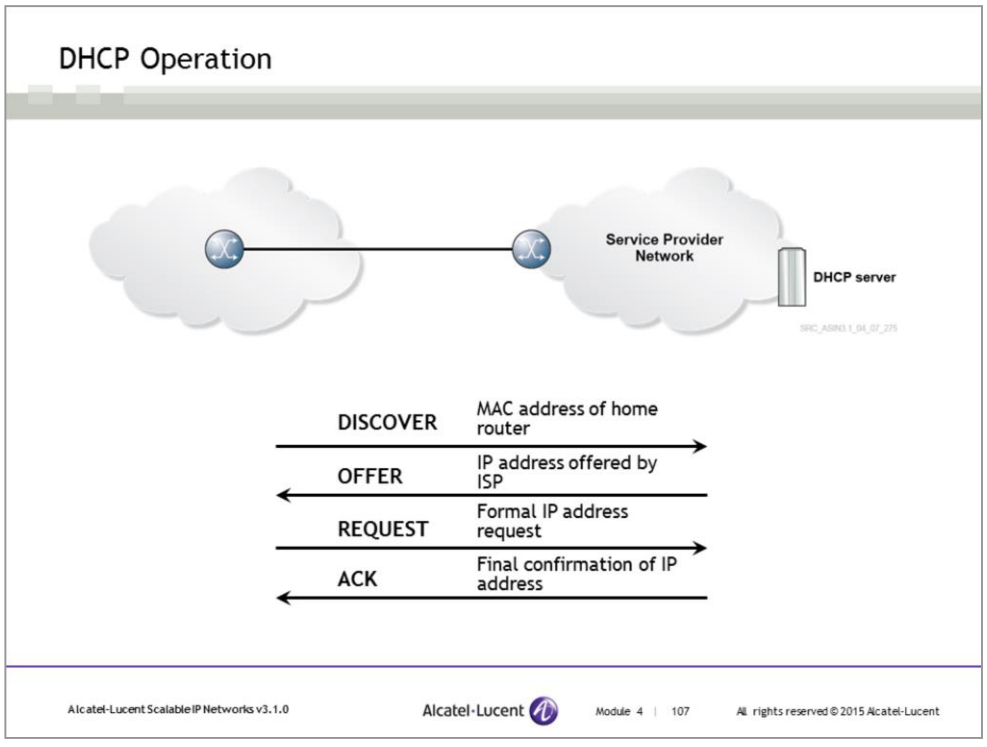
A home user does not request an IP address from the IANA, instead the user requests an IP address from a service provider. The service provider is assigned IP address blocks depending on its size and business requirements, and supply its customers with addresses for their use. A home address is typically assigned a dynamic single IP address or multiple IP addresses, depending on the service plan with its service provider.

The home router can also have a static IP address assigned by the service provider. However, in most cases the IP addresses are distributed dynamically.

If the home router uses point-to-point (PPP) to connect to the service provider, the IP address can be sent to the home router as part of the PPP session establishment. Otherwise, the home router uses Dynamic Host Control Protocol (DHCP) to get an address from the service provider.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Using DHCP, a home router can obtain an IP address automatically from the ISP. DHCP is defined in RFC 2131.

In this slide, the home user broadcasts a DISCOVER request, which is then answered by the provider DHCP server with an OFFER of an IP address. The home router then broadcasts a REQUEST with the IP address that is offered by the server. The provider DHCP server sends an ACK message to the home router, indicating that the home router can start using the IP address that was originally sent in the OFFER.

DHCP uses User Data Protocol (UDP) as its transport protocol. DHCP messages from a client to a server are sent to the 'DHCP server port' (UDP port 67). DHCP messages from a server to a client are sent to the 'DHCP client port' (UDP port 68).

The following list describes the DHCP process in detail.

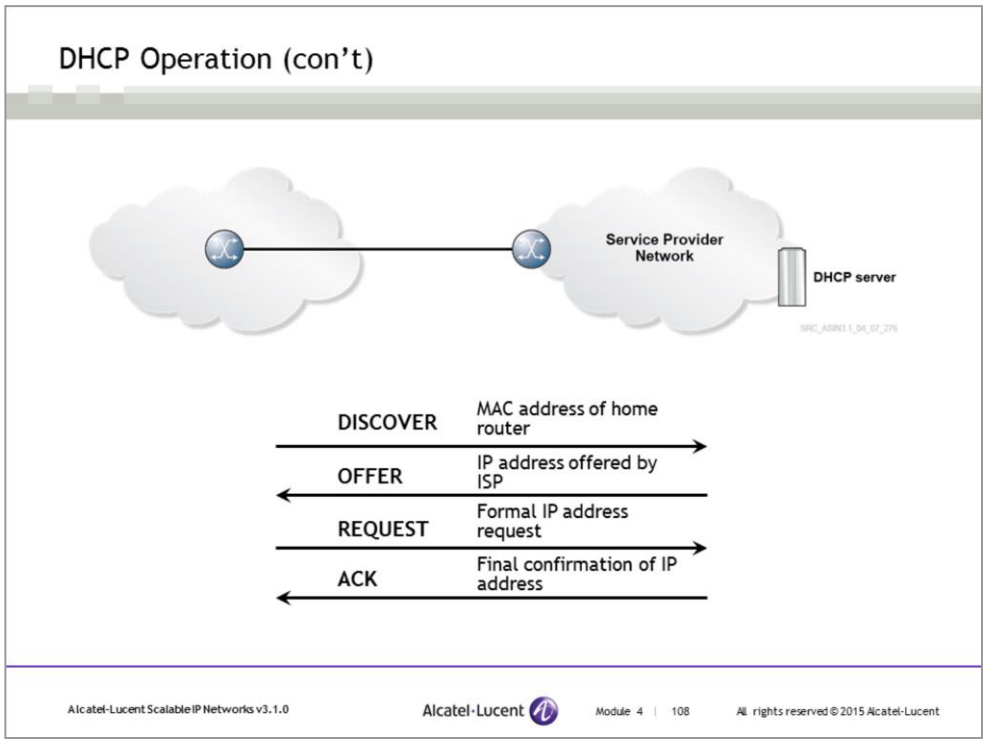
DISCOVER— The DHCP client initiates the process by broadcasting a datagram that is destined for UDP port 67. This first datagram is known as a DHCP discover message, which is a request to any DHCP server that receives the datagram for configuration information. The DHCP discover datagram contains many fields, but the most important field contains the MAC address of the DHCP client.

OFFER— A DHCP server, which is configured to lease addresses for the network that the client computer resides on, constructs a response datagram known as a DHCP offer and sends the datagram via broadcast to the computer that sent the DHCP discover. This broadcast is sent to UDP port 68 and contains the MAC address of the DHCP client. The DHCP offer also contains the MAC and IP addresses of the DHCP server, and the values for the IP address and subnet mask that are offered to the DHCP client.
At this point, the DHCP client can receive several DHCP offers, assuming there are multiple DHCP servers with the capability to offer the DHCP client an IP address. In most cases, the DHCP client accepts the first DHCP offer that arrives.

(…continued on next slide)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



(…continued from previous slide)

REQUEST— The client selects an offer, and constructs and broadcasts a DHCP request datagram. The DHCP request datagram contains the IP address of the server that sent the offer and the physical address of the DHCP client. The DHCP request performs two basic tasks. First of all, the request informs the selected DHCP server that the client requests the server to assign an IP address (and other configuration settings) to the DHCP client. Secondly, the request notifies the other DHCP servers with outstanding offers that their offers were not accepted.

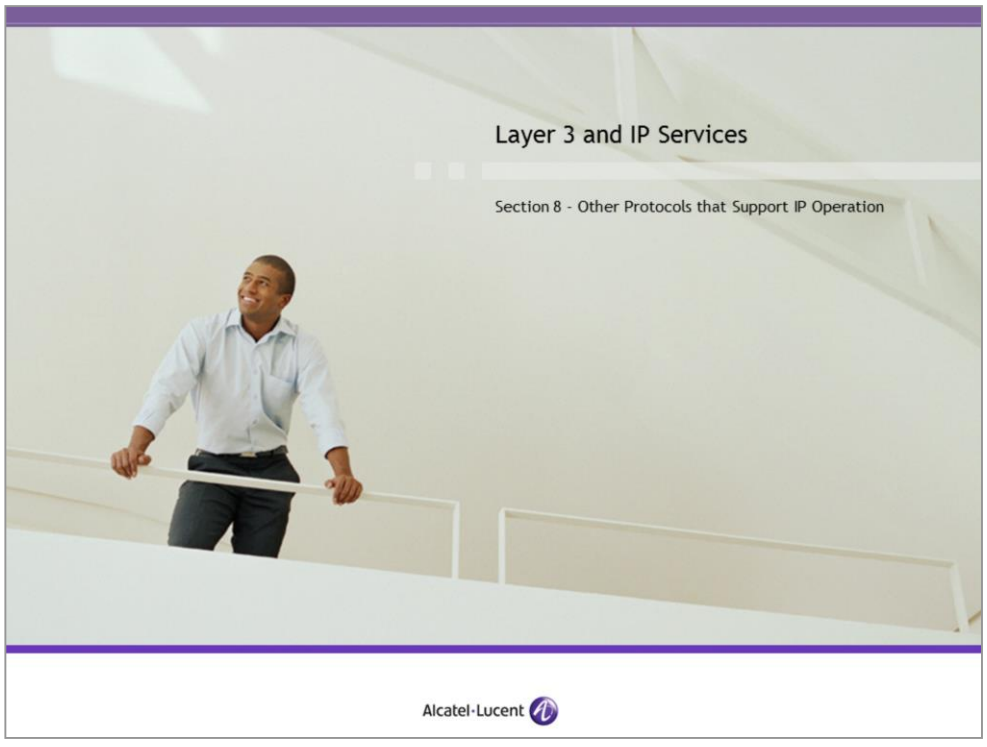
ACK— When the DHCP server from which the offer was selected receives the DHCP request datagram, the server constructs the final datagram of the lease process. This datagram is known as a DHCP ACK (short for acknowledgement). The DHCP ACK includes an IP address and subnet mask for the DHCP client. Optionally, the DHCP client is often also configured with IP addresses for the default gateway, several Domain Name Servers (DNSs), and possibly one or two Windows Information Name Servers (WINS). In addition to IP addresses, the DHCP client can receive other configuration information such as a NetBIOS node type, which can change the order of NetBIOS name resolution.

DHCP servers maintain a list of assigned IP addresses and the term of each lease. Before the lease expiration, the client that requested an IP address via DHCP requests an IP address again. The server can choose to assign a different IP address or the IP address that was previously assigned.

For a home gateway router that performs address translation, the home router performs the role of a client to the service provider. The personal router also performs the role of a DHCP server for personal devices. IP-enabled devices at home request IP addresses from the personal router, which assigns IP addresses in the private range.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

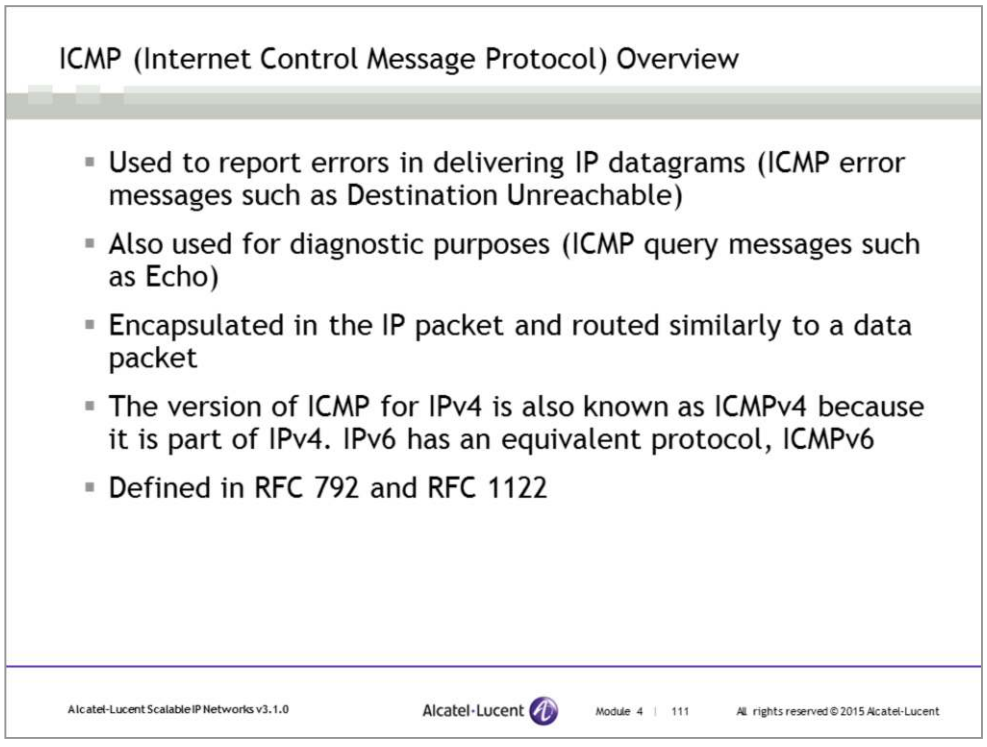
After successful completion of this section, you will be able to:

- Describe the functions and operations of ICMP
- Describe the ARP with an example of resolving an L2 address

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Internet Control Message Protocol (ICMP) messages are constructed at the IP layer, usually from a normal IP datagram that generated an ICMP response.

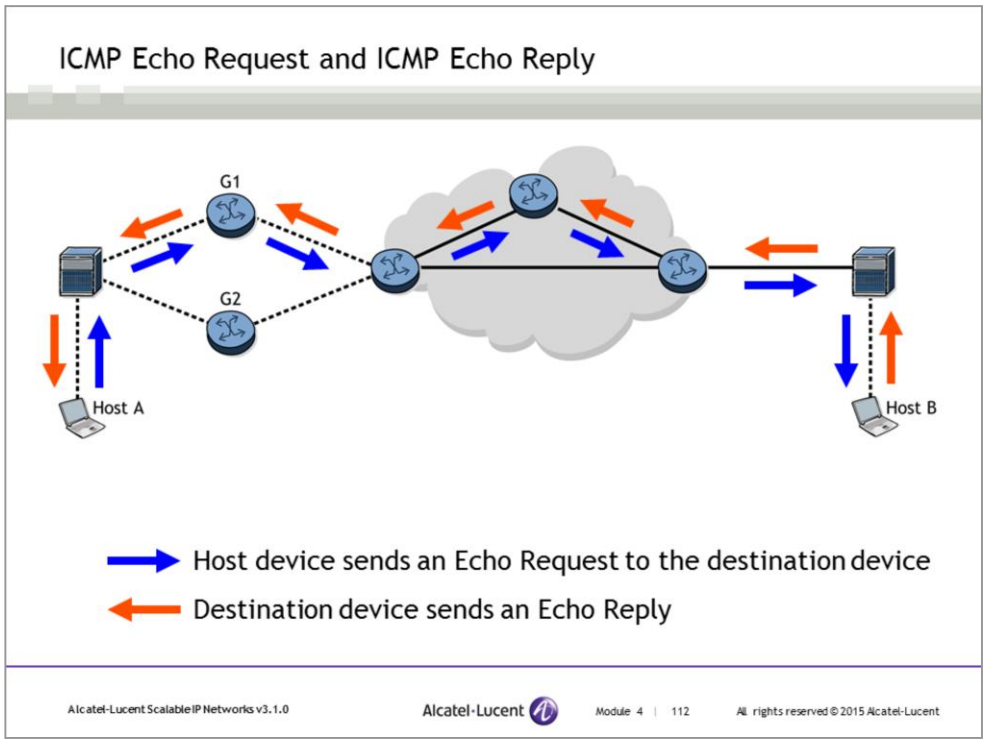
For example, each device (such as an intermediate router) that forwards an IP datagram must decrement the TTL field of the IP header by one. If the TTL reaches 0, an ICMP "time to live exceeded in transit" message is sent to the source of the datagram. IP creates the appropriate ICMP message with a new IP header (to get the ICMP message from the original sending host) and transmits the resulting datagram in the usual manner.

Each ICMP message is encapsulated directly in a single IP datagram. Therefore, as with UDP, ICMP does not guarantee delivery.

Although ICMP messages are contained in standard IP datagrams, ICMP messages are usually processed as a special case, differentiated from normal IP processing, rather than processed as a normal subprotocol of IP. In many cases, it is necessary to inspect the contents of the ICMP message and deliver the appropriate error message to the application that generated the original IP packet (that is, the application that prompted the sending of the ICMP message).

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Echo request and echo reply messages are used by well known ping applications and are very commonly used.

A host or router sends an ICMP echo request message to a specified destination. Any device that receives an echo request generates an echo reply and returns the reply to the original sender. The echo request contains an optional data area, and the echo reply contains a copy of the data sent in the request. The echo request and reply can, therefore, be used to test whether a destination is reachable.

The use of the echo request and echo reply allows for a very simple test of network connectivity. In order for the echo request and echo reply to be received, the following network conditions must be true, which gives a quick and easy way to determine if a network is correctly forwarding IP packets:

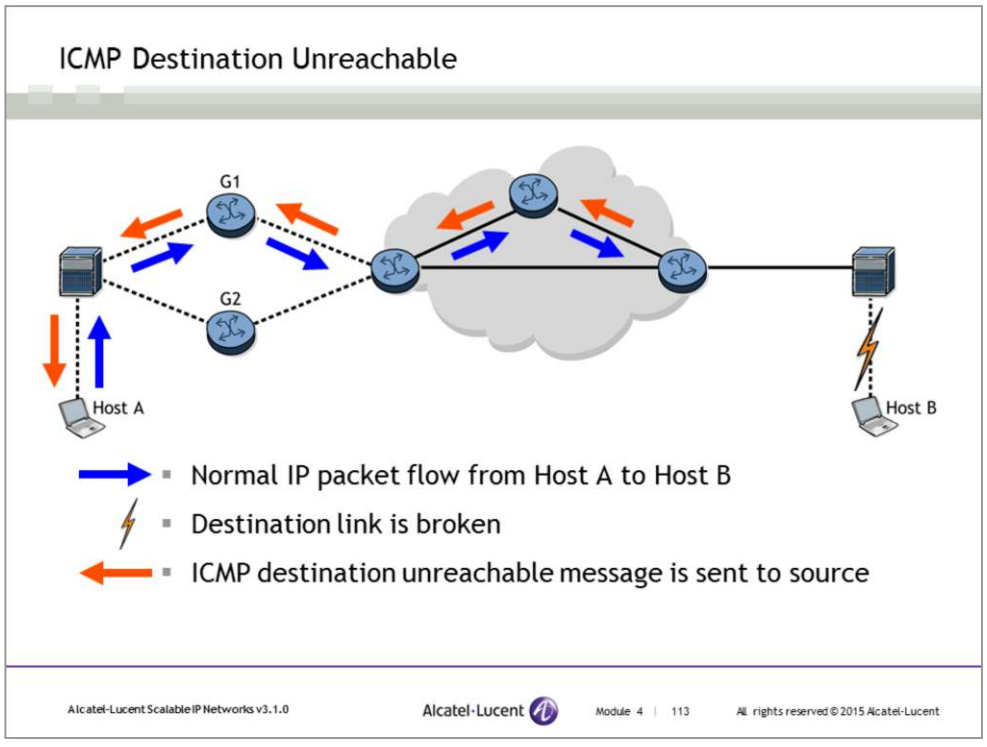
- The IP software on the source computer must route the datagram.
- The intermediate routers between the source and destination must be operating and must route the datagram correctly.
- The destination device must be running, and both the ICMP and IP software must be working.
- All routers along the path must have the correct routes.

In this slide, Host A can determine if Host B is on the network and processing IP datagrams by sending an echo request command to Host B's IP address. The echo request is routed through the network to Host B, which then sends an echo reply message back to Host A's IP address.

The ping application is the most common way to send an ICMP echo request and receive an ICMP echo reply. The command usually sends a series of echo request messages and captures the corresponding echo replies. The ping application then calculates the data return time and data loss statistics.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The destination unreachable message is used to inform the sending host that the destination address cannot be reached. For example, if the destination device is connected to an Ethernet network, the network hardware does not provide ACKs. Therefore, a router can continue to send packets to a destination even after the destination is powered down without receiving an indication that the destination is down.

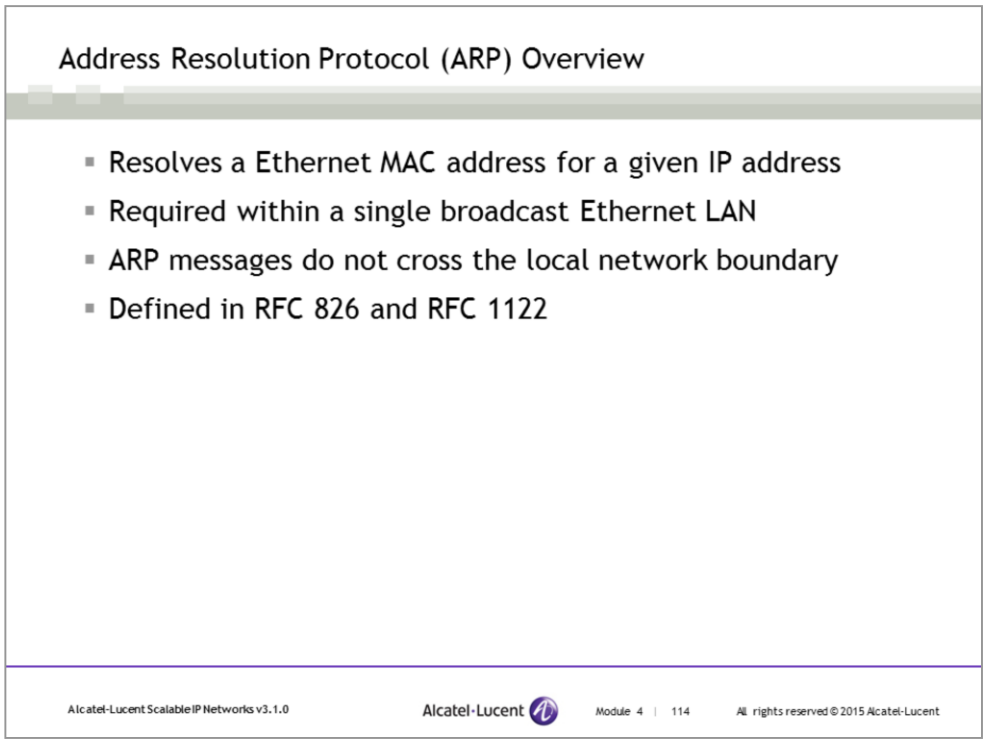
The destination unreachable message contains a code field that provides additional information as to why the packet was not delivered. For example:

- If a router does not have a route to the destination network, the router will return destination unreachable, code 0 (network unreachable).
- If the router connected to the destination network does not receive a reply to its ARP request for the destination address, the router will send a destination unreachable code 1 (host unreachable).
- If the packet must transit a network where the MTU is less than the IP datagram size and the DF flag (Don't Fragment) is set in the IP header, the router drops the packet and returns a destination unreachable code 4 (fragmentation required and DF flag set).

In this slide, Host A is attempting to send packets to Host B, but Host B is no longer available. Without an ICMP message, it is up to Host A's upper-layer protocols to time-out the connection. As an alternative, if the network link to Host B is down, a router can send an ICMP destination unreachable message to Host A so that it can inform the upper-layer protocols.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



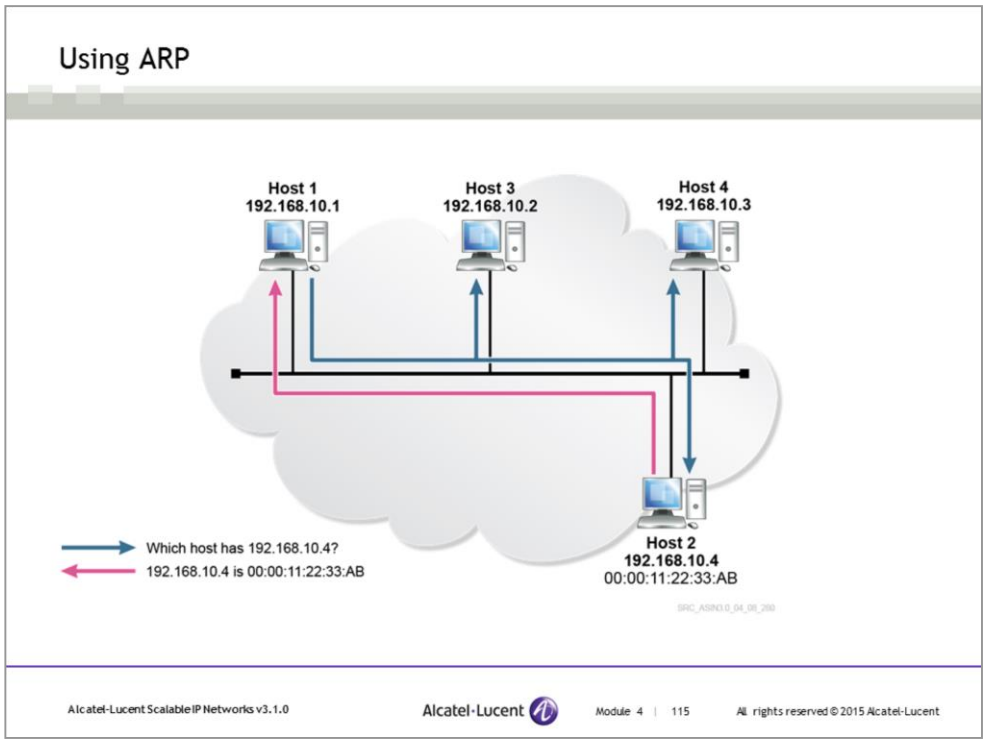
The Address Resolution Protocol (ARP) is defined in RFC 826. However, RFC 826 contained some ambiguities that were clarified in RFC 1122 (Host Network Requirements). Therefore, ARP implementations need to incorporate both RFC 826 and RFC 1122 in order to work reliably and consistently with other implementations.

RFC 826 introduced the concept of an ARP as a useful way for devices to locate the Ethernet hardware address of another IP host on the same local network. All Local Area Network (LAN) media and many Wide Area Network (WAN) media now use ARP to locate the hardware addresses of other IP devices on the local network.

When a device needs to send an IP packet to another device on the local network, the IP software first checks whether it knows the hardware address associated with the destination IP address. If so, the sender transmits the data to the destination system, using the protocols and addressing appropriate for the network medium used by the two devices. However, if the destination system's hardware address is not known, the IP software must locate the address before any data can be sent. At this point, IP uses ARP to locate the hardware address of the destination system.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



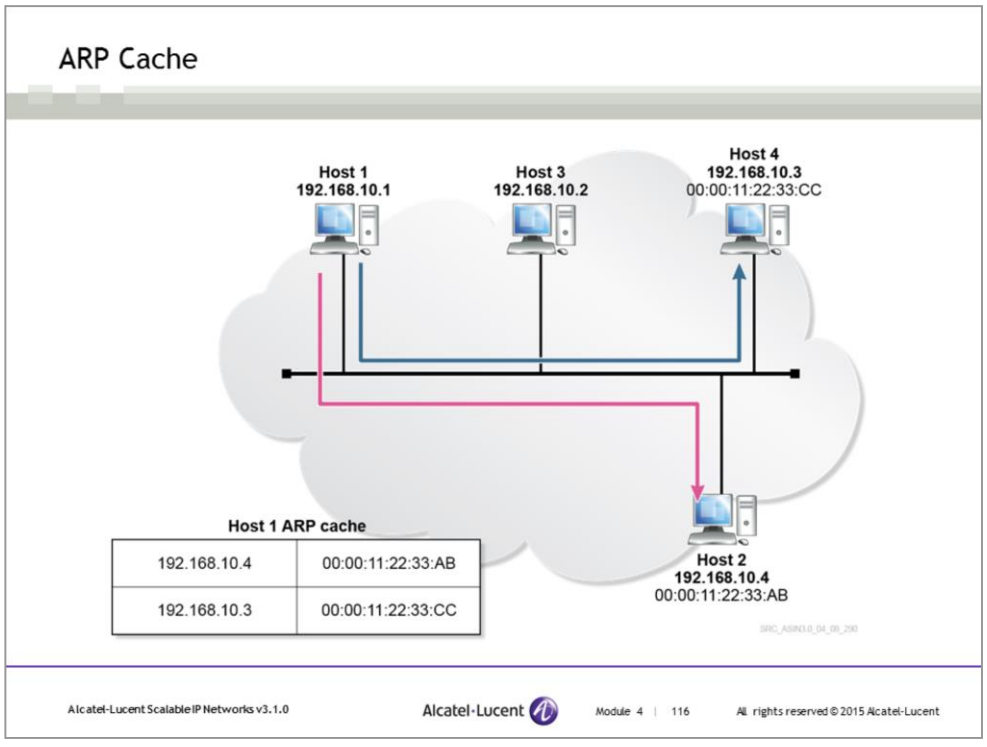
ARP performs this task by sending an IP broadcast to the network, requesting (ARP request) the system that is using the specified IP address to respond with its hardware address. If the destination system is powered up and on the network, the system will detect this broadcast (as will all of the other devices on the local network), and will return an ARP response to the original system. Note that the response is not broadcast over the network, but is sent directly to the requesting system.

All of the local IP devices must monitor the network for ARP broadcasts and, if they detect a request for themselves (as indicated in the destination IP address field of the ARP request), the devices must generate a response packet and send the packet to the requesting system. The response packet consists of the local device's IP and hardware addresses. The response is also marked as such, with the message-type field indicating that the current packet is an ARP response. The new ARP packet is then unicast directly to the original requester, where the packet is received and processed.

In this slide, Host 1 tries to ping Host 2. Host 1 checks its cache of MAC addresses for the destination MAC address of Host 2. If the MAC address is not in the cache, Host 1 sends an ARP request message. The ARP request is a broadcast message that is sent to all hosts in the broadcast domain. Each host opens the frame and checks the destination IP address. If the address is not the host's address, the host ignores the packet. However, when Host 2 receives the request with its own IP address, it sends an ARP reply. This ARP reply is carried in a frame that has for its destination the MAC address of Host 1, and the source is the MAC address of Host 2. When the reply is received, Host 1 learns the MAC address of Host 2 and can now transmit the ICMP message in a frame with the MAC address to Host 2.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When the requesting system receives an ARP response, the system stores the hardware and IP address pair of the requested device in a local cache. The next time that the system needs to send data, the system will check the local cache and, if an entry is found, the system will use the entry, which eliminates the need to broadcast another request.

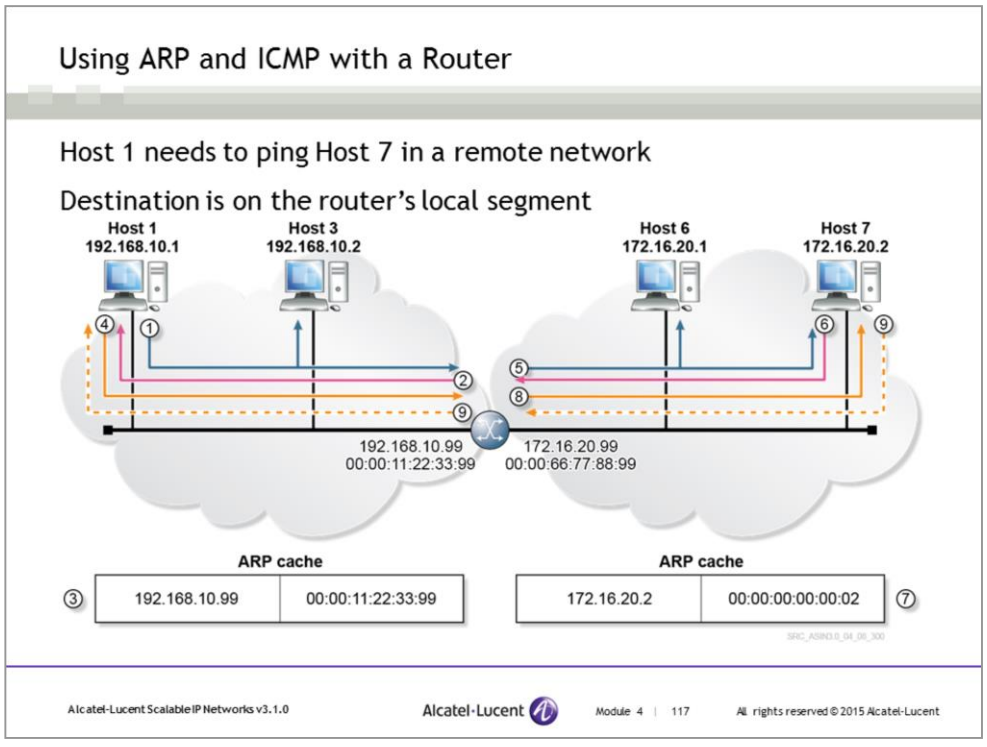
Similarly, the system that responded to the ARP broadcast will store the hardware and IP addresses of the system that sent the original broadcast. If it did not do so, it would have to issue its own ARP broadcast for Host 1's MAC address to find out where to send the ICMP echo response, which would create unnecessary network traffic. Note that IP addresses assigned to a host may not be static and can move around from host to host (recall earlier discussion of DHCP). Therefore, if the ARP cache is not timed out, the source may be unable to send its traffic to the correct destination host. Several strategies exist that can alleviate the situation, but they are outside the scope of this course.

In order to reduce the number of ARP requests, IP hosts maintain an ARP cache that contains the answer to previous ARP requests. The entries in the ARP cache are saved for a limited amount of time and then discarded.

In this slide, Host 1 maintains an ARP cache that has the MAC addresses for Hosts 4 and 2. Therefore, Host 1 does not need to send an ARP request for these hosts. However, if Host 1 needs to send traffic to Host 3, Host 1 will use ARP to get Host 3's hardware/MAC address and then insert the addresses in its ARP cache.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



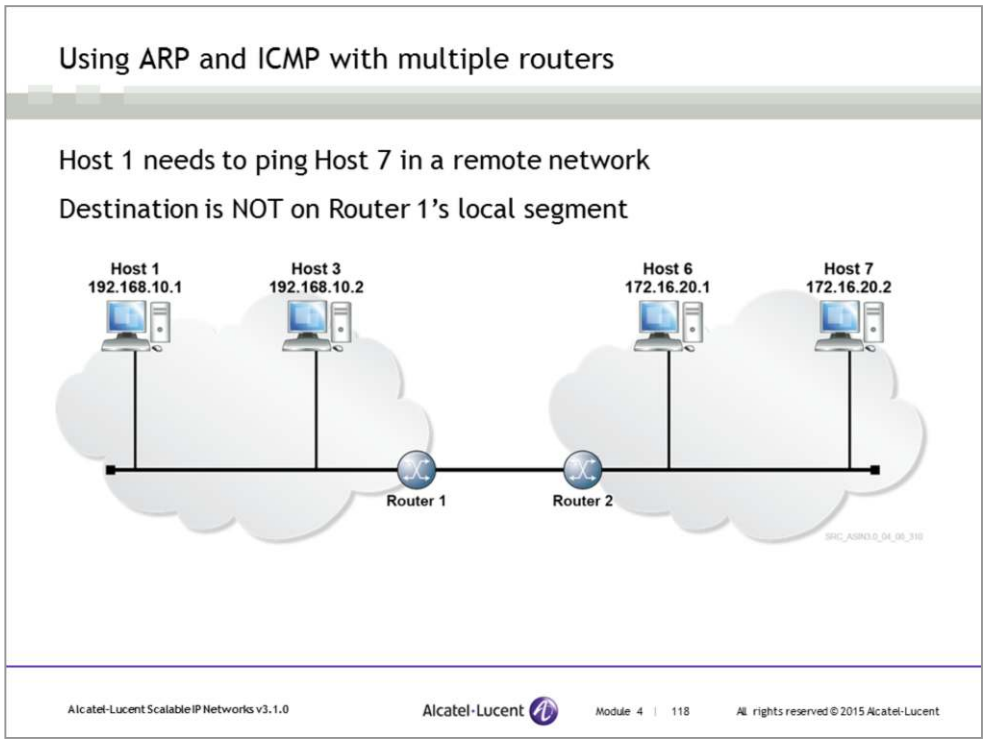
In the previous slide, we discussed the use of the ARP in the same subnet. What happens if the distant host is not in the same subnet, as shown in this slide?

Host 1 wants to ping Host 7, which is in a remote broadcast domain. Because 172.16.20.2 is not in the local subnet, Host 1 must send the frame to its default gateway to reach to the final destination. The router responds with its MAC address, and Host 1 sends the ICMP echo request to the router for forwarding.

1. Host 1 sends an ARP request for its default gateway - the router interface.
2. The router receives the broadcast on its interface in the 192.168.10.0 domain and sends an ARP response with its MAC address.
3. The MAC address of the router interface is stored in Host 1's ARP cache.
4. Host 1 can now send the IP packet containing the ICMP Echo Request with a destination address 172.16.20.2 to its default gateway.
5. The router uses its forwarding table and determines that the destination is on a local segment. However, the router does not have an ARP entry for the host 172.16.20.2. Therefore, the router sends an ARP request including the destination IP address to that specific segment, 172.16.20.2, in this broadcast domain.
6. When Host 7 receives the broadcast, it responds with a unicast ARP response to the router.
7. The router stores the MAC address of Host 7 in its ARP cache.
8. The router can now send the IP packet containing the ICMP Echo Request to Host 7.
9. Host 7 responds with an Echo Response addressed to Host 1. Because Host 7 has the MAC address of the router interface in its ARP cache, and the router has the MAC for Host 1, no more ARP broadcasts are required. The packet is sent hop-by-hop from Host 7 to the router and on to Host 1.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In the previous slide, we discussed ARP's use within the router's local segment. What happens if the distant host is not in the router's local segment, as shown in this slide?

Host 1 wants to ping Host 7, which is in a remote broadcast network. Because 172.16.20.2 is not in the local subnet, Host 1 must send the frame to its default gateway to reach the final destination. The router responds with its MAC address, and Host 1 sends the ICMP echo request to the router for forwarding.

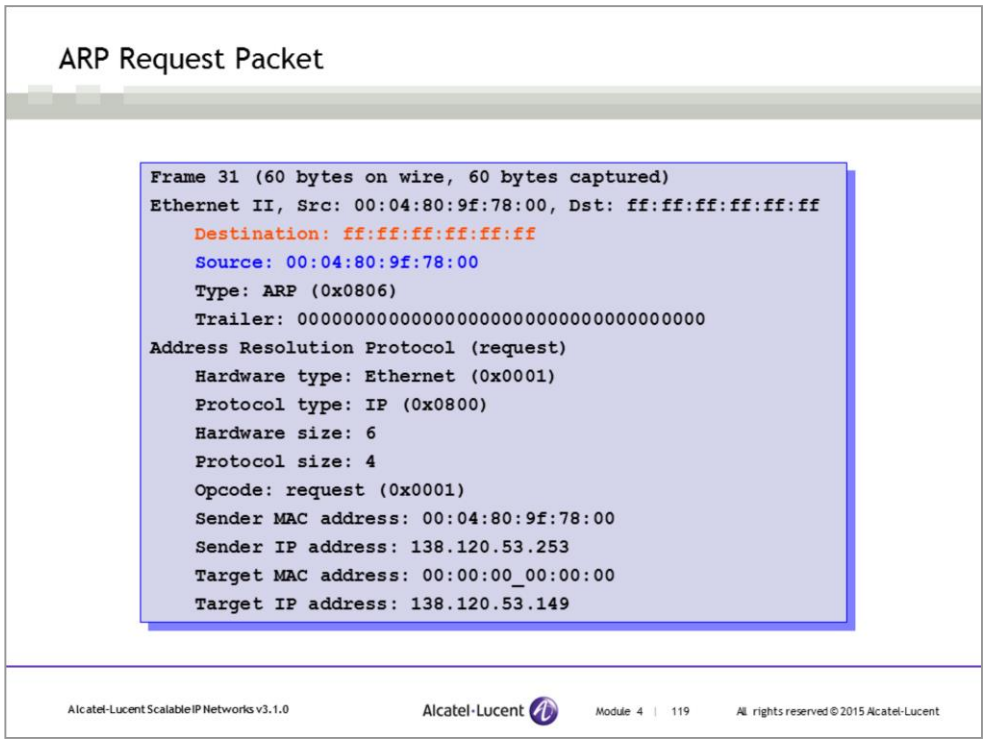
1. Host 1 sends an ARP request for its default gateway – Router 1's interface.
2. The router receives the broadcast on its interface in the 192.168.10.0 network and sends an ARP response with its MAC address.
3. The MAC address of the router interface is stored in Host 1's ARP cache.
4. Host 1 can now send the IP packet containing the ICMP Echo Request with destination address 172.16.20.2 to its default gateway, Router 1.
5. Router 1 uses its forwarding table to determine that the destination is NOT on its local segment. Router 1 needs to forward the ICMP Echo Request to the next hop, which is Router 2's interface address. Since Router 1 does not have an ARP entry for Router 2's interface address, Router 1 sends an ARP request to the interface connecting Router 2.
6. Router 2 receives the ARP request and responds to Router 1 with a unicast ARP response.
7. Router 1 stores the MAC address of Router 2's interface and sends the IP packet containing the ICMP Echo Request with destination address 172.16.20.2 to Router 2.
8. Router 2 checks its forwarding table and determines that the destination is on its local segment. However, Router 2 does not have an ARP entry for Host 7. Router 2 sends an ARP request to that specific segment.
9. When Host 7 receives the ARP request, it responds with a unicast ARP response to Router 2.
10. Router 2 stores the MAC address of Host 7 in its ARP cache.
11. Router 2 can now send the IP packet containing the ICMP Echo Request to Host 7.
12. Host 7 responds with an Echo Response addressed to Host 1. Because Host 7 has the MAC address of Router 2 in its ARP cache, Router 2 has the MAC address of Router 1, and Router 1 has the MAC address for Host 1, no more ARP broadcasts

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

are required. The packet is sent hop-by-hop from Host 7 to Router 2, to Router 1, and on to Host 1.

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



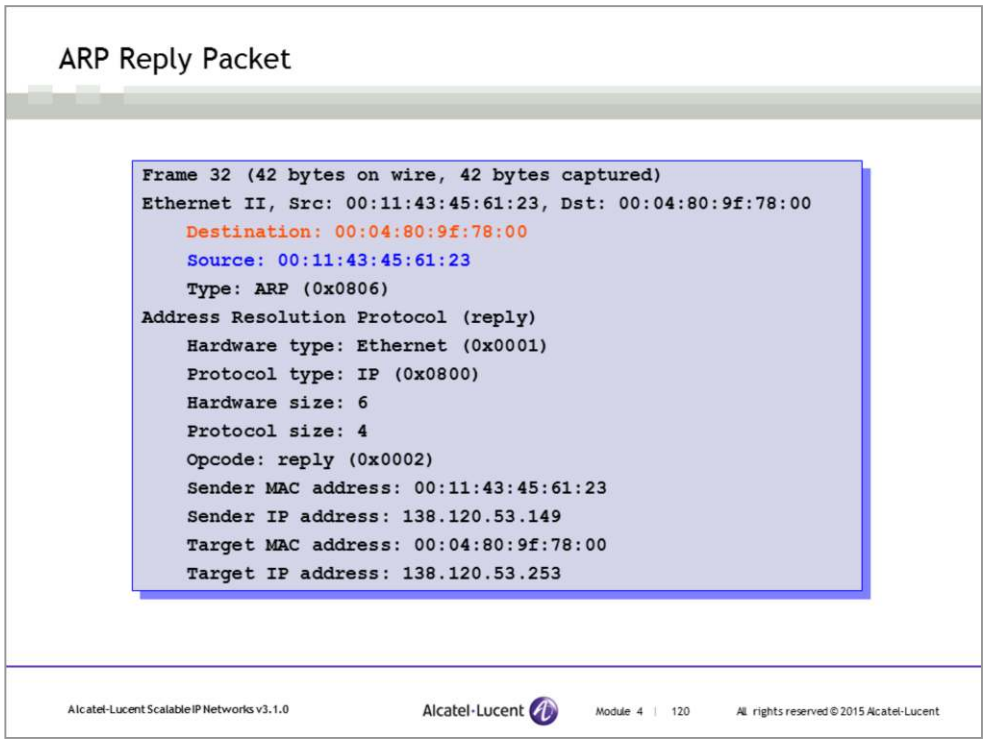
This slide shows a packet capture of an ARP request. The capture shows a host with IP address 138.120.53.253 that is attempting to resolve the MAC address for a host with IP address 138.120.53.149. The destination MAC address of the Ethernet II frame is sent to the broadcast address ff:ff:ff:ff:ff:ff. All devices in the same broadcast domain will receive this frame. Only the host with IP address 138.120.53.149 will reply. For ARP, the type is 0x0806 and indicates which protocol is transported in the Ethernet II frame.

The fields in the ARP packet include:

- Hardware type - Each L2 protocol is assigned a number that is used in this field; for example, Ethernet is 1.
- Protocol type - Each protocol is assigned a number that is used in this field; for example, IP is 0x0800.
- Hardware size – Size in bytes for hardware addressing. Ethernet addresses are 6 bytes.
- Protocol size – Size in bytes for logical addressing. IPv4 addresses are 4 bytes.
- Opcode (Operation Code) - Operation that the sender is performing. A value of 1 is for an ARP request, and a value of 2 is for an ARP reply.
- Sender MAC address - MAC address of the sender.
- Sender IP address – The protocol address of sender.
- Target MAC address - Hardware MAC address of the intended receiver. The MAC address will be all 0's for a request.
- Target IP address - Protocol address of the intended receiver.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

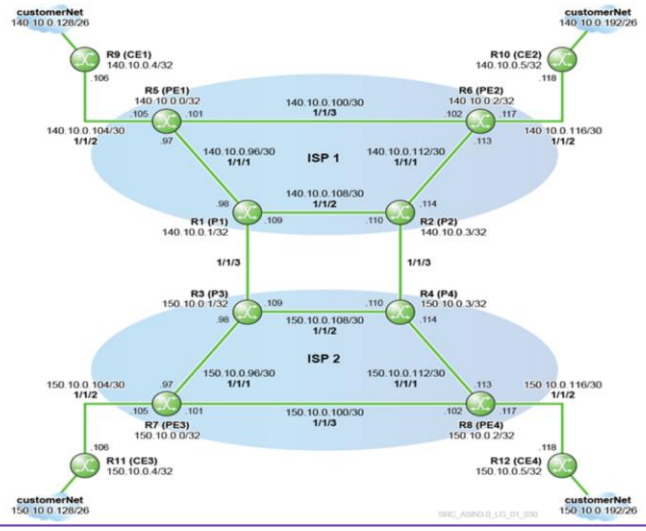


This slide shows the packet capture of an ARP reply in response to the ARP request on the previous slide. The Ethernet frame is a unicast frame and is sent only to the MAC address of the ARP request sender. All of the fields in the ARP reply packet have the same meaning as the fields in the ARP request packet. The main differences in the APR reply packet are: the Opcode (value 2 is for request) and the packet contains MAC addresses for the sender and the target. Note that the sender and target addresses have been swapped.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

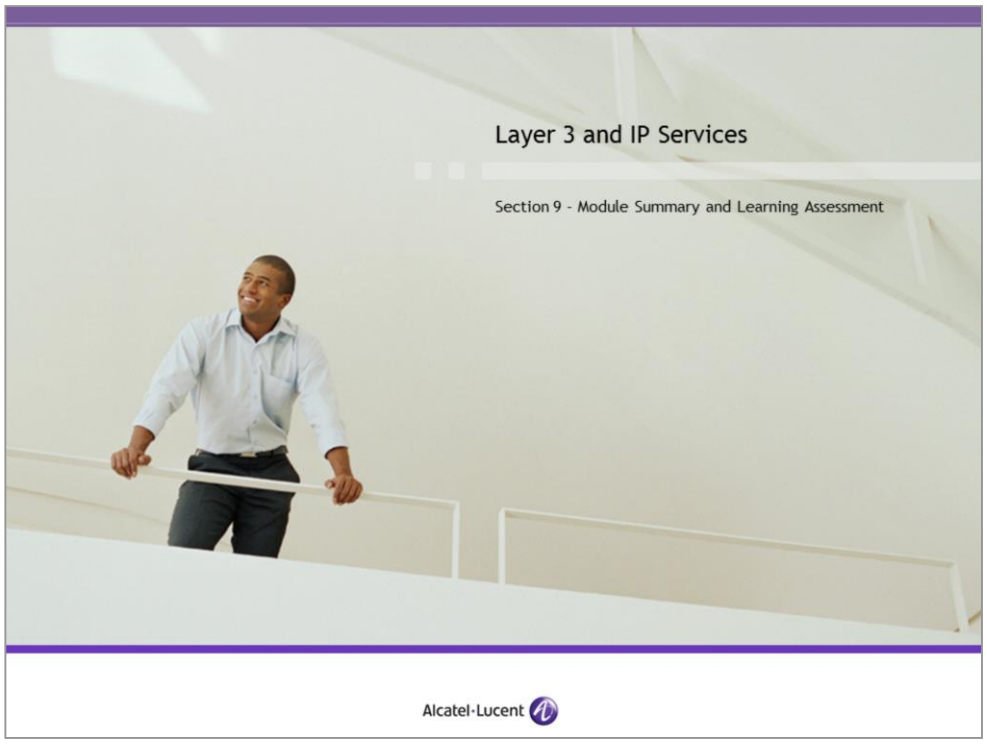
Lab 2.3 ICMP and ARP Operation



 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Summary

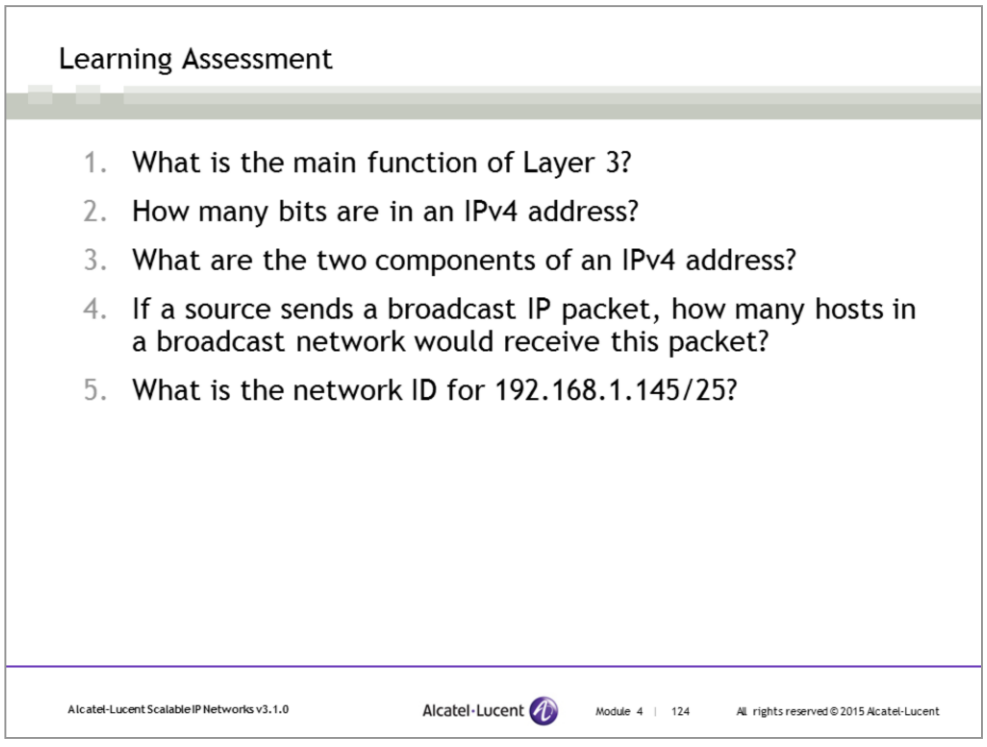
After successful completion of this module, you should be able to:

- Describe Layer 3 and IP services
- Describe the basics of IP addressing, including its components, classes, how they are managed and allocated, and the purpose and types of addresses
- Describe the purpose, components, and operation of the IP subnet address
- Develop an IP address plan using IP subnetting and addressing summarization
- Recognize and define the fields in the IP header
- Describe the IP address forwarding process
- Describe other protocols that support IP operation

 All rights reserved © 2015 Alcatel-Lucent

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

1. What is the main function of Layer 3?

The main function of Layer 3 (L3) is to move data from the source to its destination, or set of destinations, regardless of where the destination exists. L3 performs this function by using a unique logical address and a standard set of protocols to help forward data based on the addressing scheme. Although a number of L3 protocols are still in use, Internet Protocol (IP) is used almost exclusively today.

2. How many bits does an IPv4 have?

32 bits

3. Name the two components of an IPv4 address and explain what they do.

The first component of an IP address, known as the network number or network prefix, identifies the network that a host resides in.

The second component of an IP address, known as the host number, identifies an individual host inside that network.

4. If a source sends a broadcast IP packet, how many hosts in an IP network would receive this packet?

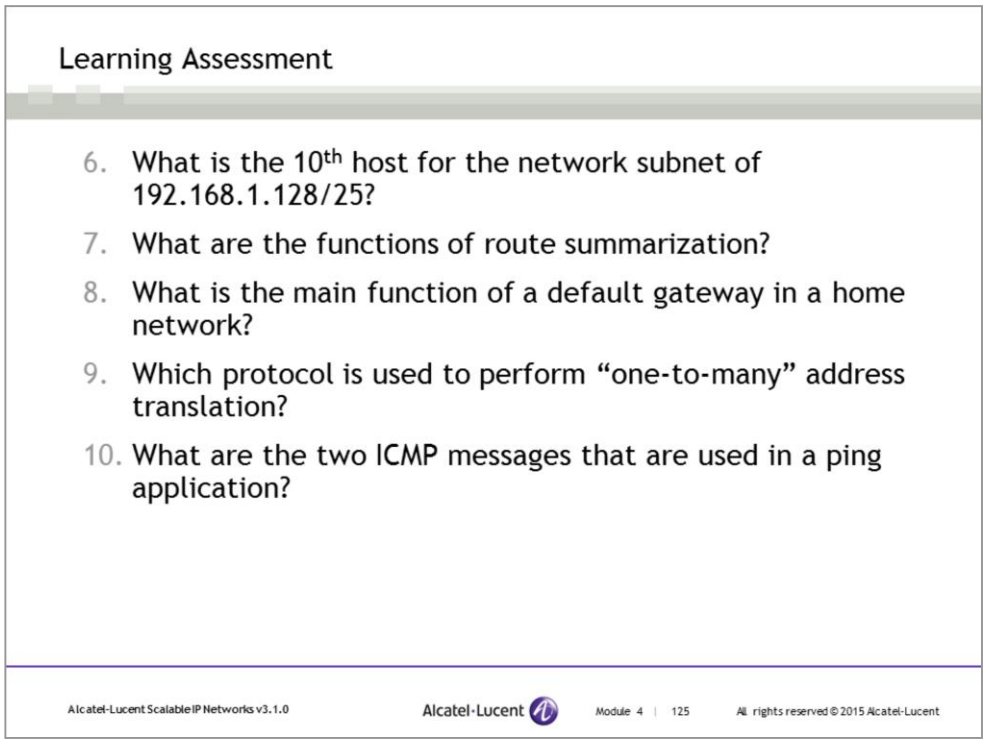
All hosts in a broadcast network.

5. What is the network ID for 192.168.1.145/25?

With a network prefix length of 25, the first 25 bits (3 octets + 1 bit) are the network portion. The network ID for the first three octets would be the same as the IP address, which is 192.168.1. The last octet of the IP address (145) is binary 10010001. The last octet of the IP address mask is binary 10000000. The last octet of the network ID is the result of the operation 10010001 AND 10000000, which is binary 10000000 (128). Therefore, the network ID is 192.168.1.128.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

6. What is the 10th host for the network subnet of 192.168.1.128/25?

The 10th host is 192.168.1.128 + 10, which is 192.168.1.138.

7. What are the functions of route summarization?

To group a number of route entries with a common prefixes into a single entry in the routing table; to reduce the number of route entries to be advertised by the router; to increase routing advertisement stability.

8. What is the main function of a default gateway in a home network?

Allows home/personal devices to access other devices on the Internet.

9. Which protocol is used to perform "one-to-many" address translation?

Port Address Translation (PAT) performs "one-to-many" translation. One public IP address can support multiple private IP addresses simultaneously.

10. What are the two ICMP messages that are used in a ping application?

ICMP Echo Request and ICMP Echo Reply.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

Module Objectives

After successful completion of this module, you will be able to:

- Explain the concepts and purpose of IP routing
- Explain the purpose and configuration of static routes
- Describe the basic concepts of a dynamic routing protocol
- Describe the purpose and basic operation of OSPF and BGP
- Describe IP filter operation, components, configuration, and application

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 2
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

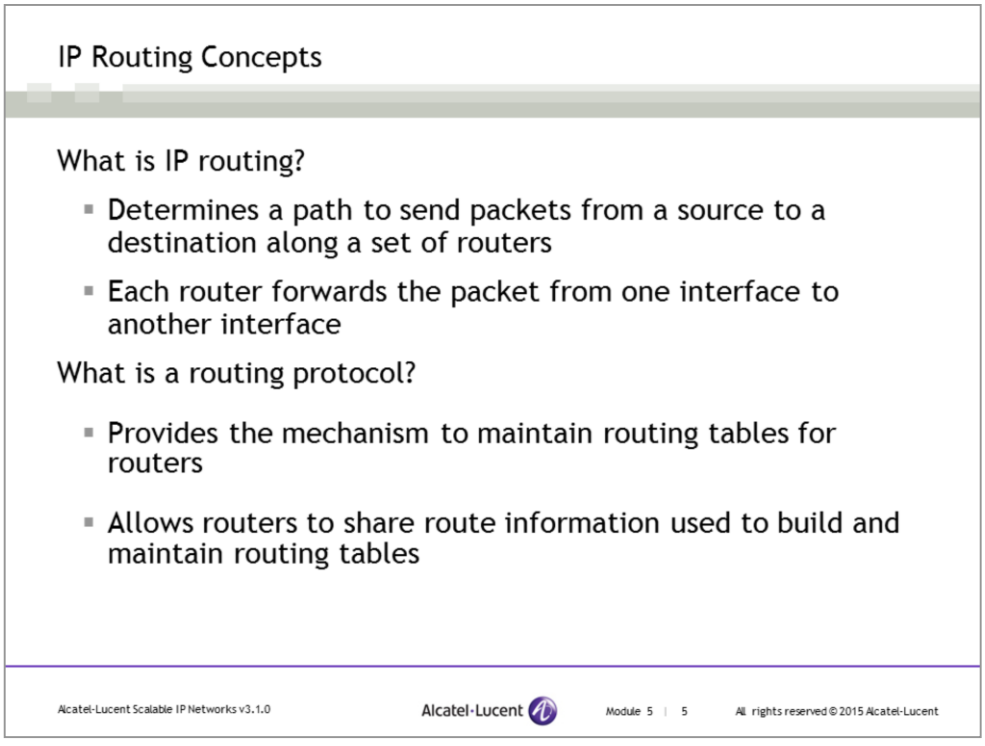
After successful completion of this section, you will be able to:

- Describe the function of the routing table
- List the methods used to populate routing table (directly connected, static, dynamic)
- Explain how RTM builds a routing table

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 4
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IP routing

IP routing is the set of tasks involved in sending a packet from the source to the destination across an IP network. The packet enters the IP network via a router and is sent to another router in the network and so on until the packet reaches the destination. The routers in the network use their routing tables to determine how to forward the packet.

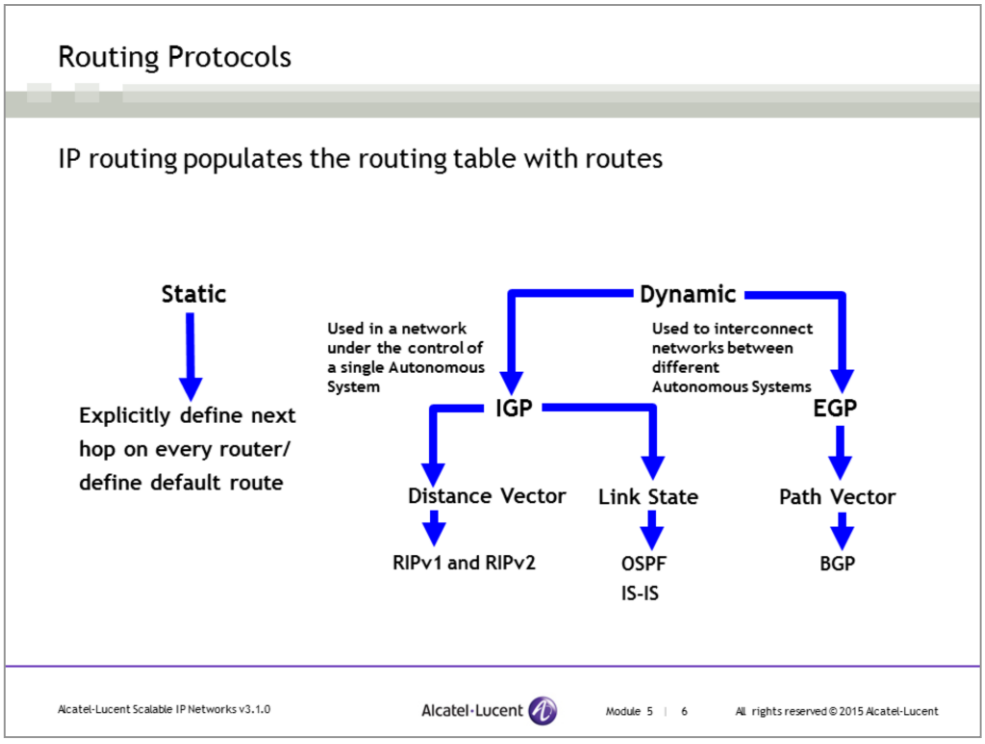
Routing tables

The routing tables are built manually by the network administrator or by protocols that run on every router.

The routing table maintains a list of IP networks and the physical interfaces on the router to reach these networks. Using the routing table, an IP packet is routed to its destination.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IP routing can be divided into two main categories - *static* and *dynamic*. Dynamic routing protocols can be further divided into two main categories - Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). The principal difference is the administrative scope of the routing protocol. IGP is intended for use in a network that is under the control of a single entity or administrative group. This single network entity is usually referred to as an Autonomous System (AS). An EGP is used to interconnect networks in different ASs.

IGPs such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS) are used for routing within an autonomous system. The goal of an IGP is to find the lowest-cost route to every destination in the network. IGPs can be further divided into *distance vector* and *link-state* protocols.

Distance vector routing protocols use a hop-count metric to determine the best route to a destination, regardless of the bandwidth capability of the network links along the path. RIP is a distance vector protocol. Routers that participate in a distance vector routing protocol do not have a complete topological view of the network; the routers only know the best next hop to the destination.

Link-state routing protocols use a cost metric that is a representation of the link status and the physical bandwidth of the router interfaces along the path. Therefore, the link-state protocols select a path based on the route that has the least cost, which is representative of the path that has the most physical bandwidth. Common link-state protocols are OSPF and IS-IS. Each router that participates in a link-state routing protocol has a complete topological view of the network.

The goal of an EGP is to provide routes between autonomous systems. However, the EGP must also consider policy enforcement that may exist between the autonomous systems. Because an EGP works within policy constraints, the protocol will not necessarily choose the lowest-cost route. BGPv4 is the current EGP used in the Internet. BGP is a path vector protocol that chooses the path based on the number of autonomous systems that must be traversed rather than on the number of routers that the path must traverse. BGP performs policy-based routing because policies can be used

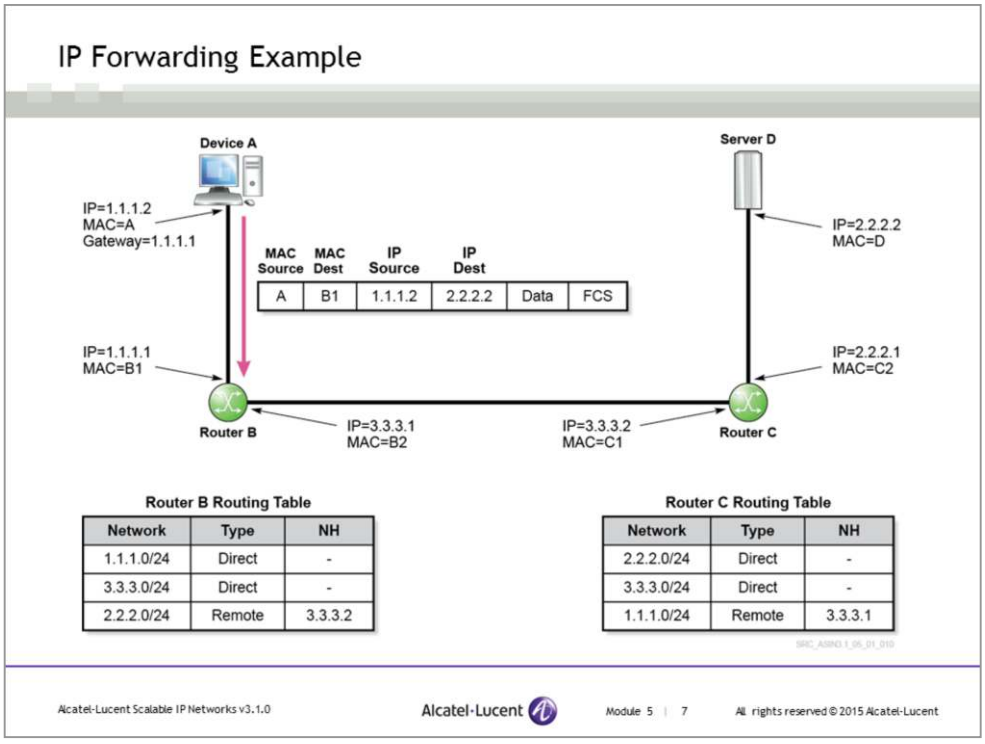
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

in many different ways to influence the ways a preferred route is chosen.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

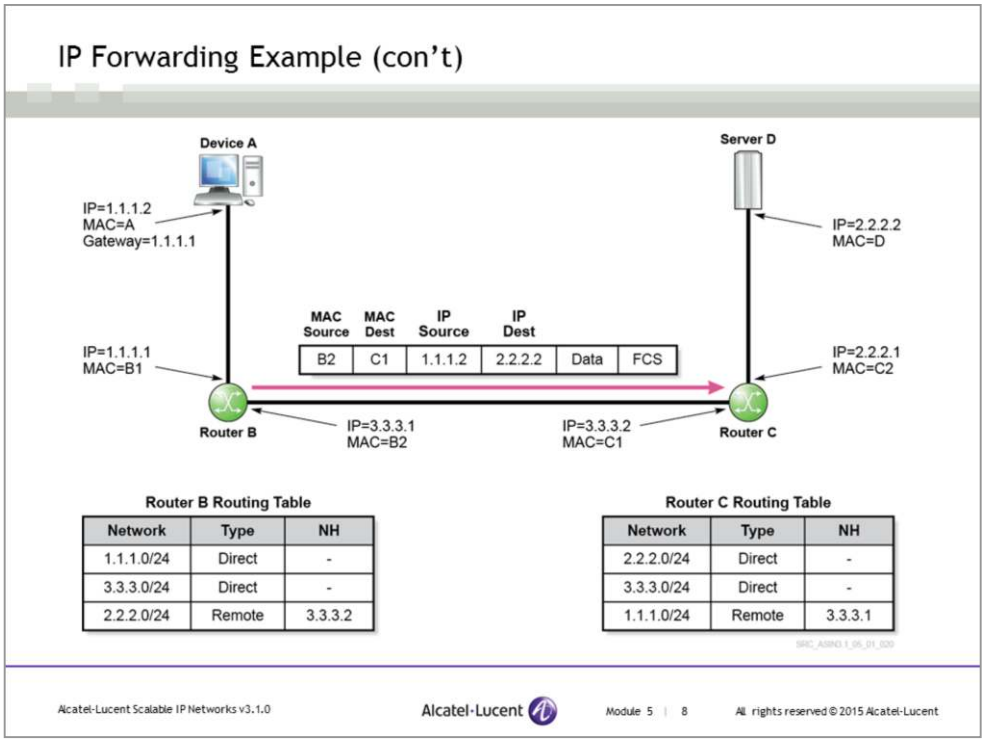


Assuming the routing tables exist on the routers in this slide, the basic flow of a data packet through a network is described in the next few slides.

First, Device A (1.1.1.2) needs to send data to Server D (2.2.2.2). Because Device A is not located on the same Local Area Network (LAN) segment as Server D, Device A must use the default gateway (1.1.1.1) for the segment. Device A uses Address Resolution Protocol (ARP) for the 1.1.1.1 address to learn the MAC address of the gateway. The router responds with the MAC B1 address. Device A can now encapsulate the data, as shown in this slide. Note that the source and destination IP addresses identify the overall source and destination devices; the frame source and destination MAC addresses identify the path across one Ethernet segment.

All rights reserved © 2015 Alcatel-Lucent

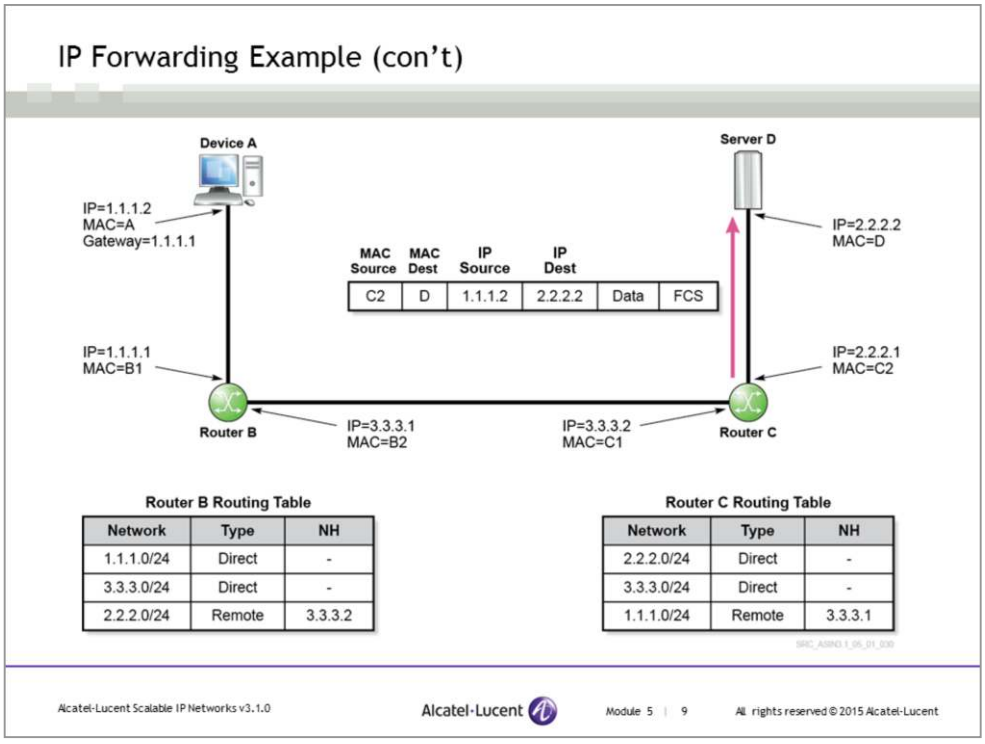
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When the frame arrives at Router B, the router removes the Ethernet header and trailer, examines the IP header, checks the routing table for an entry that has the longest match to the destination IP address in the IP packet. The matching route entry identifies that the packet needs to be sent to Router C. Router B determines this by finding the entry for the 2.2.2.0/24 network in its routing table and getting the next hop (NH) value, which in this case is 3.3.3.2 (an interface on Router C). To send the data, Router B encapsulates the data in an Ethernet frame and forwards the data.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

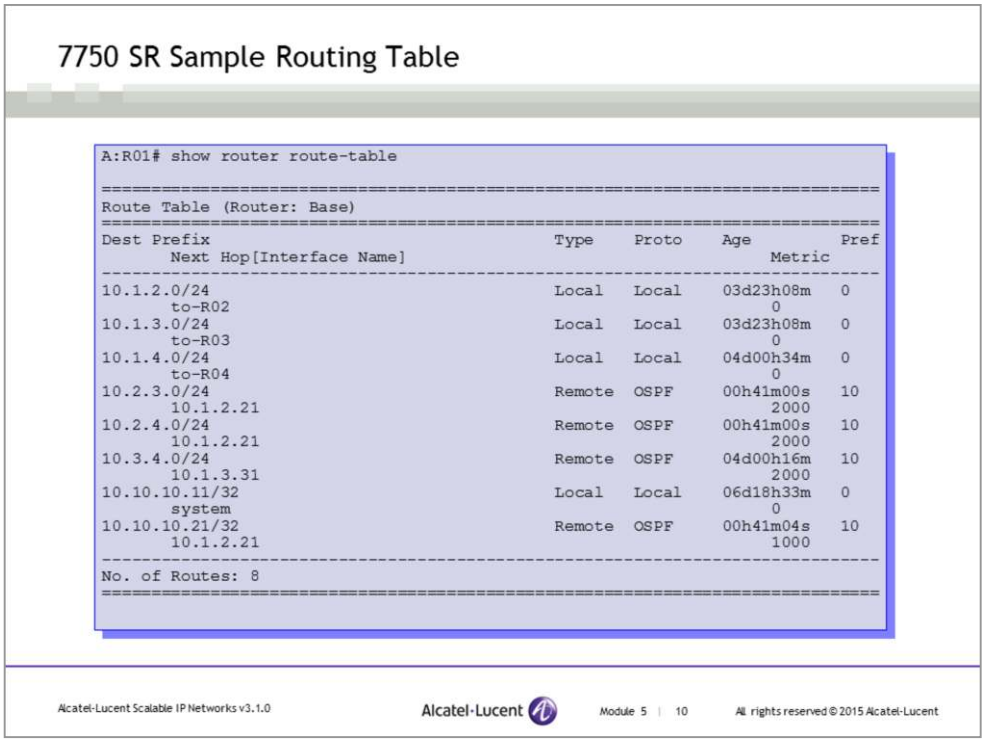


Router C removes the Ethernet frame from the IP packet and checks its routing table. Because the destination IP network is directly connected to its Ethernet port, Router C checks its ARP cache to find the destination MAC address. Note that network 2.2.2.0/24 shows as "Direct" in Router C's routing table. When the destination Ethernet MAC address is determined, Router C creates the frame of data and forwards the data to Server D.

Note that the IP addressing did not change. However, the L2 (Ethernet) framing changed over each segment that the packet traversed. The IP address identifies a device within the entire network topology; the L2 address identifies a device on that segment only.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide displays the output from an Alcatel-Lucent 7750 SR routing table.

Major components of the routing table

Dest Prefix - The network that has been advertised to this router. The terms prefix and network are used interchangeably.

Type – The type of interface. Indicates whether the destination prefix belongs to a locally attached network or to a remote network.

Protocol - If the destination network is directly attached to the router, the routing protocol will be displayed as Local. If the destination network is not directly attached to the router, the routing protocol that was used to advertise the destination prefix to this router is displayed. The protocols can be, for example, RIP, OSPF, IS-IS, BGP, and static.

Age - How long this entry has been in the routing table.

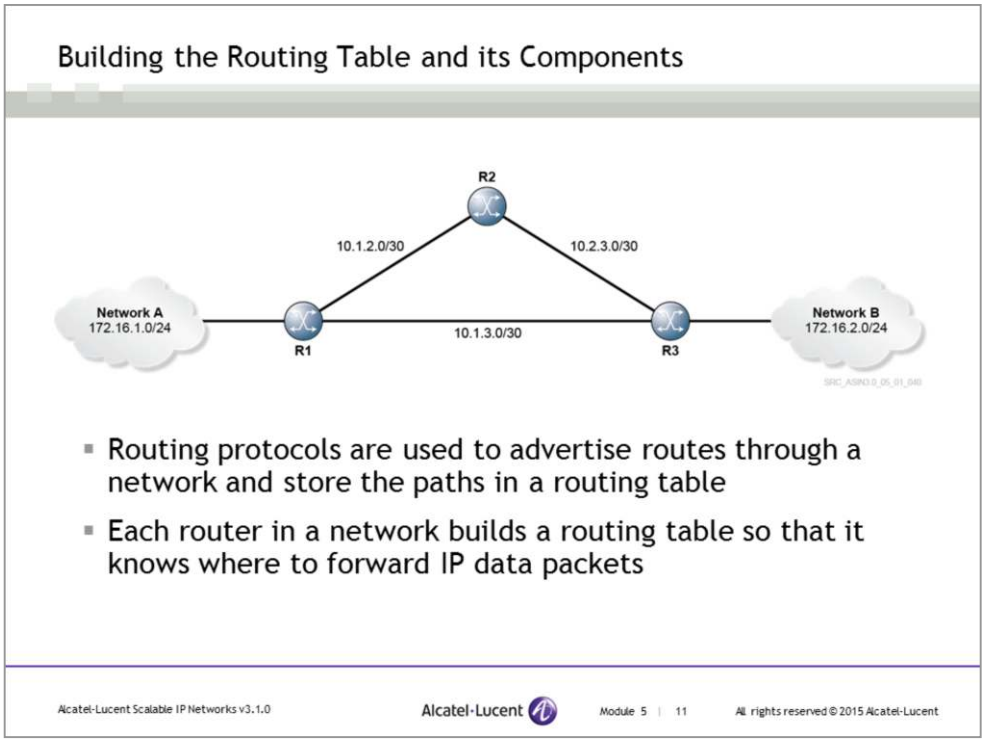
Preference - A unit of measurement that indicates the preference of one routing protocol over another routing protocol. This value is necessary in the event that the same prefix is advertised to the router from multiple routing sources.

Next Hop – Packets should be forwarded to this IP address to reach the destination prefix.

Metric - The numerical value used by a routing protocol to calculate the best route to a destination. Depending on the routing protocol, the metric is usually a hop count or a cost that is assigned to a network link. Unlike a preference, which is used to determine the preference for a route among multiple routing sources, a metric is used to determine the preferred route within a single routing protocol such as OSPF.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

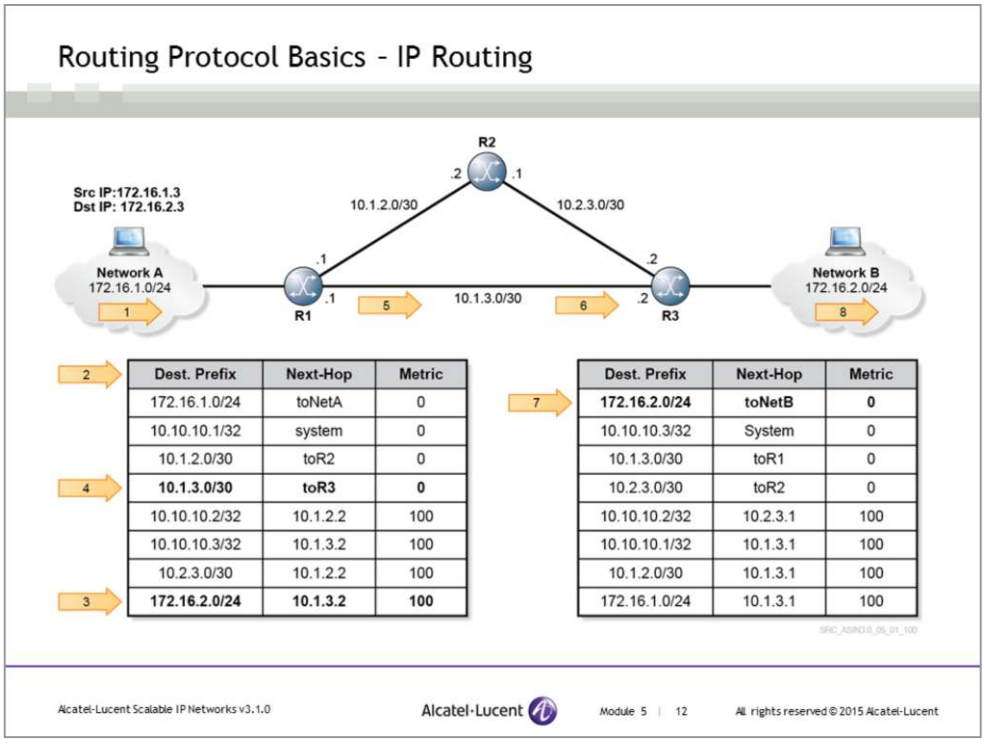


All routing protocols serve the same purpose: to find routes through a network and store the paths in a routing table. The routes are advertised to neighbors using mechanisms and procedures that are specific to each routing protocol.

Each router in a network needs to populate its routing table so that it can forward IP data packets.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



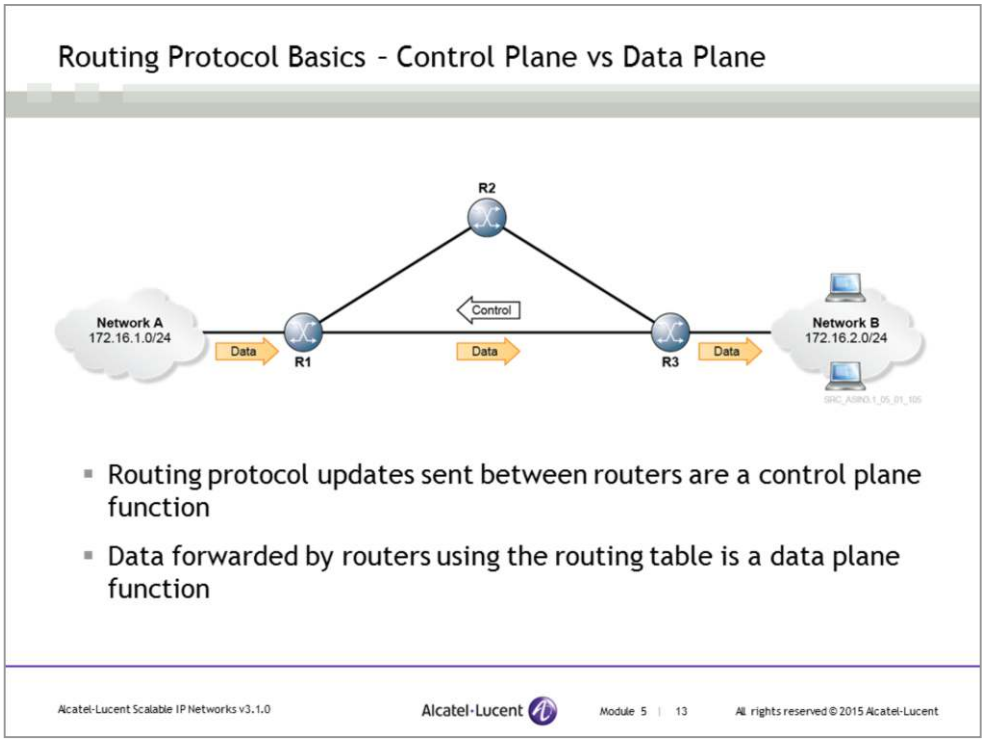
When an IP packet arrives at the ingress to router R1, R1 looks at the destination IP address and searches for a matching entry in its routing table. R1 finds a match and forwards the packet out of the appropriate interface to the next hop indicated in its routing table (router R3, in this case). R3 follows the same process as R1, determines that the route is local, and forwards the packet to its local network.

The details of the forwarding process are shown step-by-step in this slide.

1. An IP packet enters R1.
2. The IP packet's destination address is compared to the entries in the R1 forwarding table.
3. The longest entry matching the destination is found, and the next-hop IP address is examined.
4. The local interface corresponding to the next-hop IP address is then determined by re-examining the R1 forwarding table.
5. The IP packet is then forwarded to the corresponding local interface and out of R1 to its next-hop R3.
6. The IP packet enters R3.
7. R3 examines its forwarding table to find a matching destination for the IP address. It determines that the network is local and that it does not need to forward the packet to any other routers.
8. R3 puts the correct L2 header on the IP packet and forwards it to the destination device.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Modern routers such as 7750 SR have a distributed architecture that separates router functions into control plane and forwarding plane actions.

In the 7750 SR, the control plane functions, are performed by the SF/CPM (switch fabric/control plane module), and the forwarding plane fuctions are performed by the IOM cards.

Control plane functions

The control plane has two main functions:

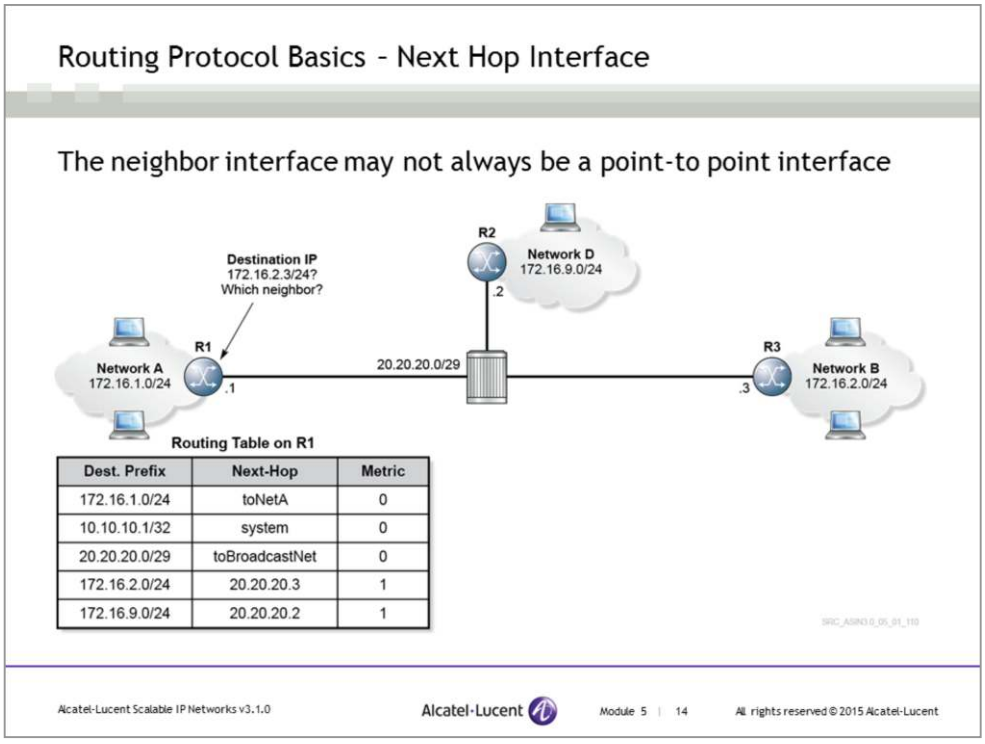
- Supporting the management functions of the router through the Command Line Interface (CLI) and network management capabilities. This includes configuration and administration of the router.
- Building the forwarding table for the IOM. The forwarding table is constructed from the routing table, which is built through the operation of dynamic routing protocols and/or configured with static routes. More information about how the forwarding table is built is discussed later in this module.

Data plane functions

The data plane functions occur after the control plane has built the forwarding information and stored the data in the IOM. The IOM cards have the intelligence and information required to forward IP packets without any involvement from the control plane. The forwarding complex on the IOM contains memory and processors that enable it to receive, process and transmit user application packets at wire speeds.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



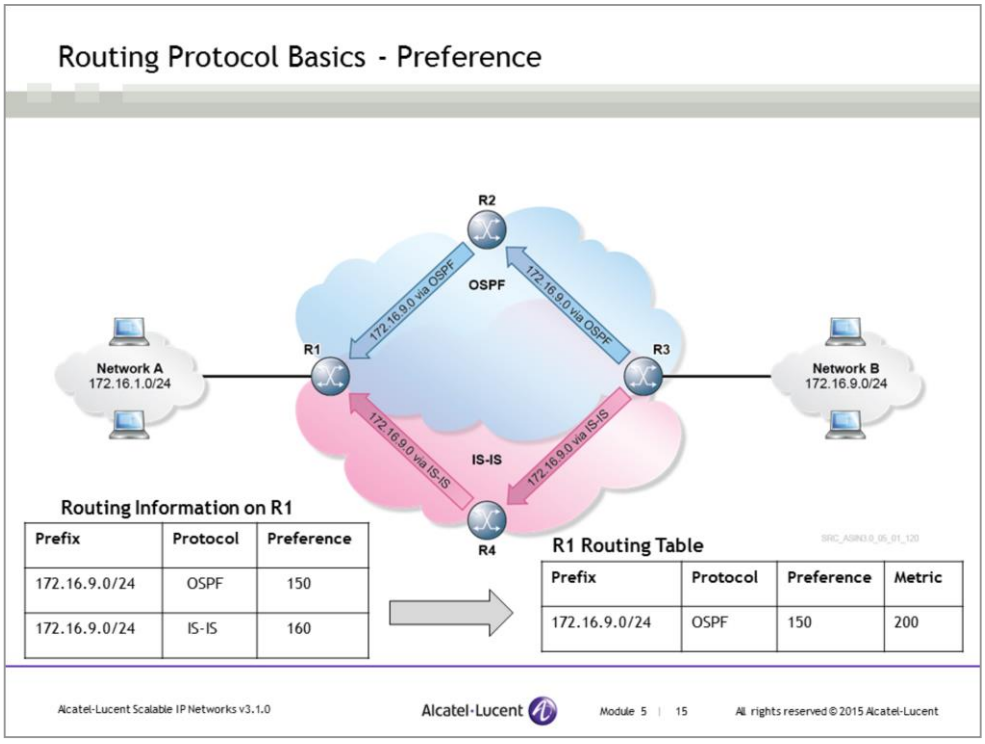
Assume routers R1, R2, and R3 are connected with a switch to form a common broadcast domain. In such cases, the process of building the IP forwarding table is the same except that R1 must use its Address Resolution Protocol (ARP) table to determine the L2 address of the next-hop routers.

In this slide R1, R2, and R3 are connected in a common broadcast domain.

- R1 has one interface that is configured towards the broadcast domain.
- When R3 and R2 send updates about their local networks to R1, they include the IP addresses of their interfaces on the broadcast domain.
- R1 installs network 172.16.9.0/24 with a next-hop of 20.20.20.2 and network 172.16.2.0/24 with a next-hop of 20.20.20.3.
- When R1 needs to send an IP packet to R2 or R3, R1 will obtain the L2 address for these routers from its ARP table and forward the packets with the correct L2 header.
- R1 needs to forward an IP packet to network 172.16.2.0/24. It examines its routing table and determines that R3 is the next hop.
- Since R3 and R1 share a common Ethernet segment, R1 will issue an ARP request for the MAC address of R3's IP address or retrieve the MAC address from its ARP table if an entry already exists for R3.
- Once R1 has the MAC address of R3, it will use this address to create the L2 header for the IP packet and forward the frame using the Ethernet protocol.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A router may run more than one routing protocol.

In this slide, the R1-R2 and R2-R3 interfaces are running OSPF, and the R1-R4 and R4-R3 interfaces are running IS-IS.

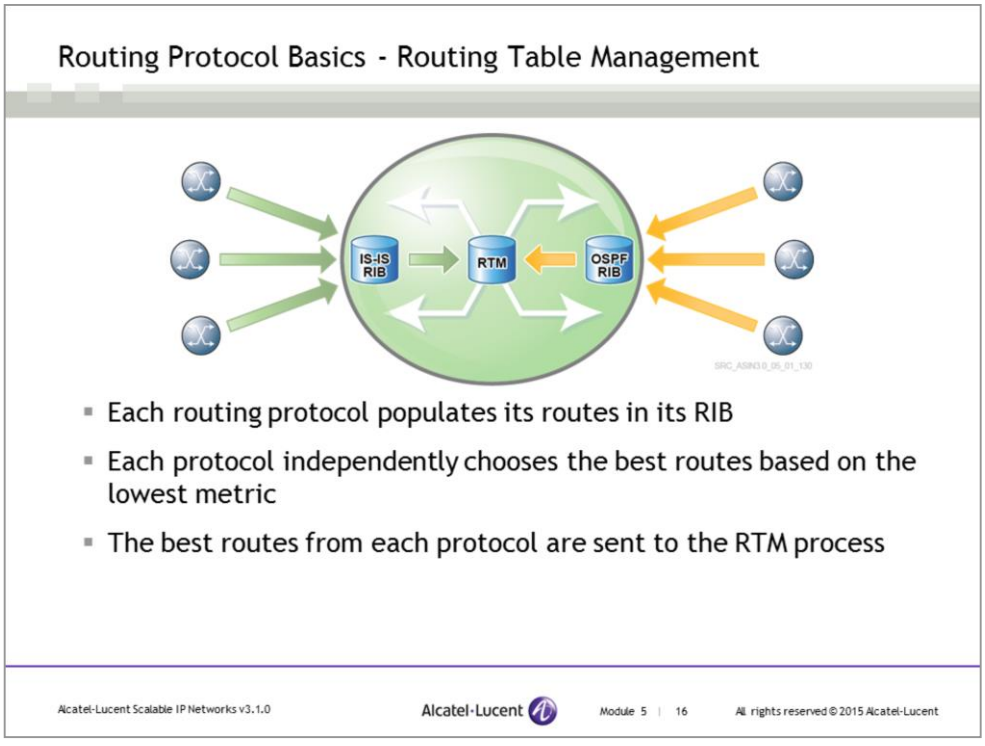
Network B can be advertised on both interfaces of R3, each running a different protocol. Therefore, this network is advertised to R1 by both IS-IS and OSPF. R1 has to decide which entry to install in its routing table. In order to choose between the two updates, R1 uses an additional parameter known as *preference*. The preference parameter indicates the router's preference of one protocol over another protocol. On the Alcatel-Lucent 7750 SR, routes learned from OSPF are preferred over routes learned from IS-IS by default. Therefore, the route learned from OSPF is installed in the routing table on R1.

Note that the protocol with a lower preference value is preferred.

These default preference values that are assigned to each routing protocol on the Alcatel-Lucent 7750 SR are listed later in this section.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

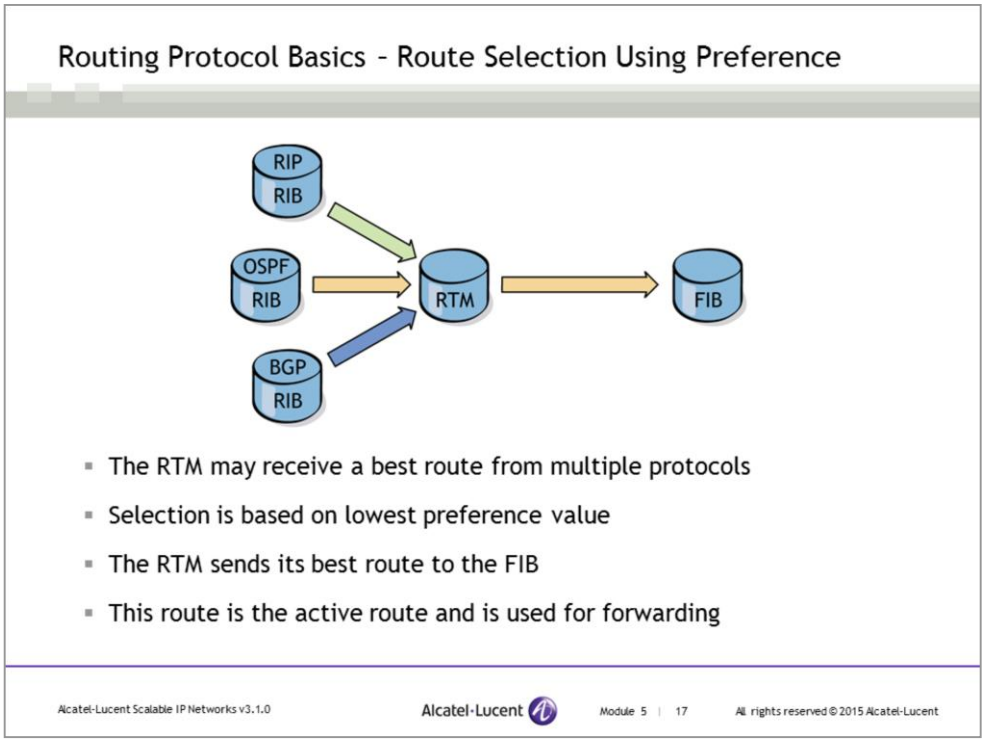


When a routing protocol learns routes from its neighbors, the protocol populates its RIBs with the routes. Each protocol stores the routes it has learned from its neighbors in its RIB.

For each destination in the RIB, the routing protocol chooses the best route based on the lowest metric. The best routes are sent to the routing table manager (RTM).

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Because metrics from different protocols are not comparable, the RTM uses the preference to choose from all of the best routes that it receives. The lower the protocol's preference, the more likely that the best or active route will be selected from that protocol.

Since the router must have a method of determining the best route, different protocols should not be configured with the same preference.

The best routes from the RTM are placed in the forwarding information base (FIB), also commonly referred to as the routing table.

The FIB is distributed to the various line cards on the Alcatel-Lucent 7750 SR and is used to forward incoming IP packets. Distributing the FIB to the line cards reduces the overall CPU processing on the router and increases the packet forwarding rate of the router.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Routing Protocol Basics - Default Preference Table

Route type	Preference	Configurable
Direct attached	0	No
Static	5	Yes
OSPF internal	10	Yes
IS-IS Level 1 internal	15	Yes
IS-IS Level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS Level 1 external	160	Yes
IS-IS Level 2 external	165	Yes
BGP	170	Yes

All rights reserved © 2015 Alcatel-Lucent

This slide lists the default preference values that are assigned to each routing protocol on the Alcatel-Lucent 7750 SR.

All of the preference values, with the exception of the preference for directly-attached networks, are configurable.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

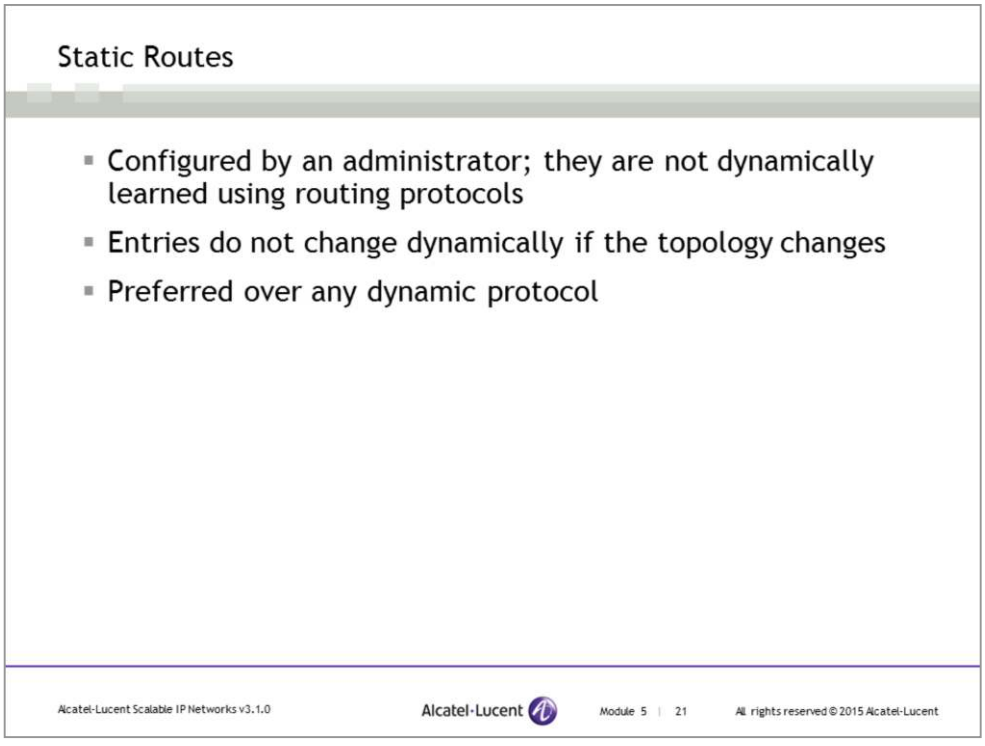
After successful completion of this section, you will be able to:

- Define static routing and default routing
- Configure a static route and a default route

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent



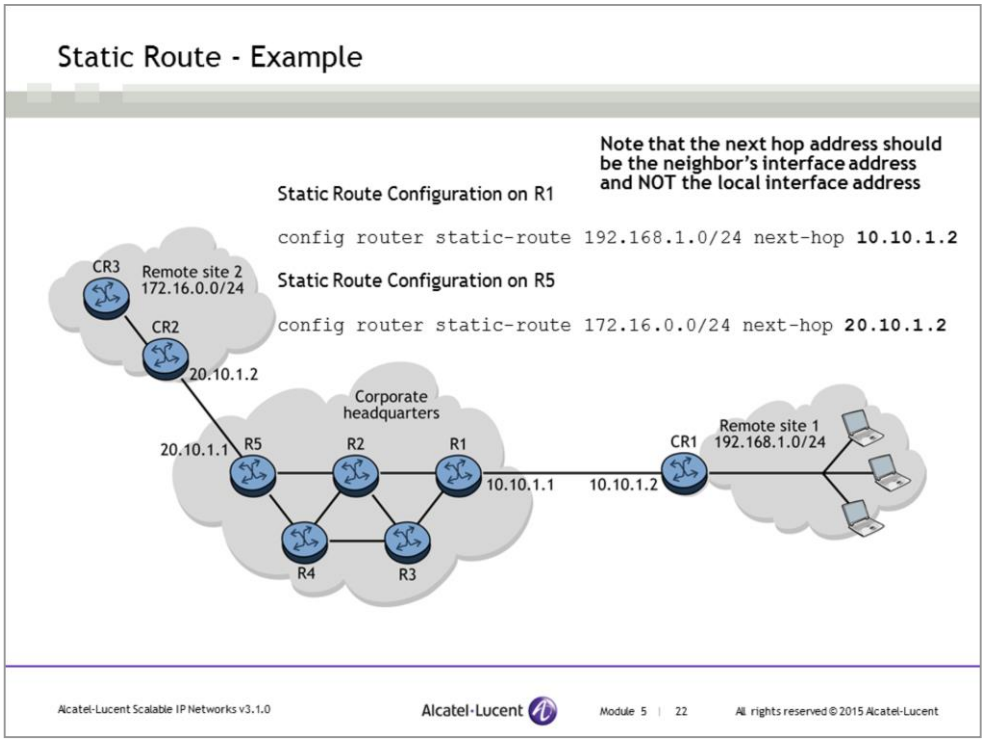
Static routes are manually configured. They describe the remote destination network and the next-hop that a packet must be forwarded to in order to reach the destination. The destination can be one network or a range of networks.

By default, a static route is created with a preference of 5 and a metric of 1. However, these parameters can be changed to accommodate a different configuration. If the preference and metric parameters are left at the default values, a static route is always preferred over a route learned from a dynamic routing protocol. By adjusting the preference value, you can define a secondary route that will be used if the dynamic protocol fails to provide a route. Or, a second static route can be configured as a backup to the primary static route by assigning a higher metric to the secondary route.

Static routing saves bandwidth and processing because there are no advertisements or updates. However, any changes to the routes must be made manually, so there is no real-time response if a destination becomes unreachable. Static routing also allows you to override any decision made due to a routing protocol.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



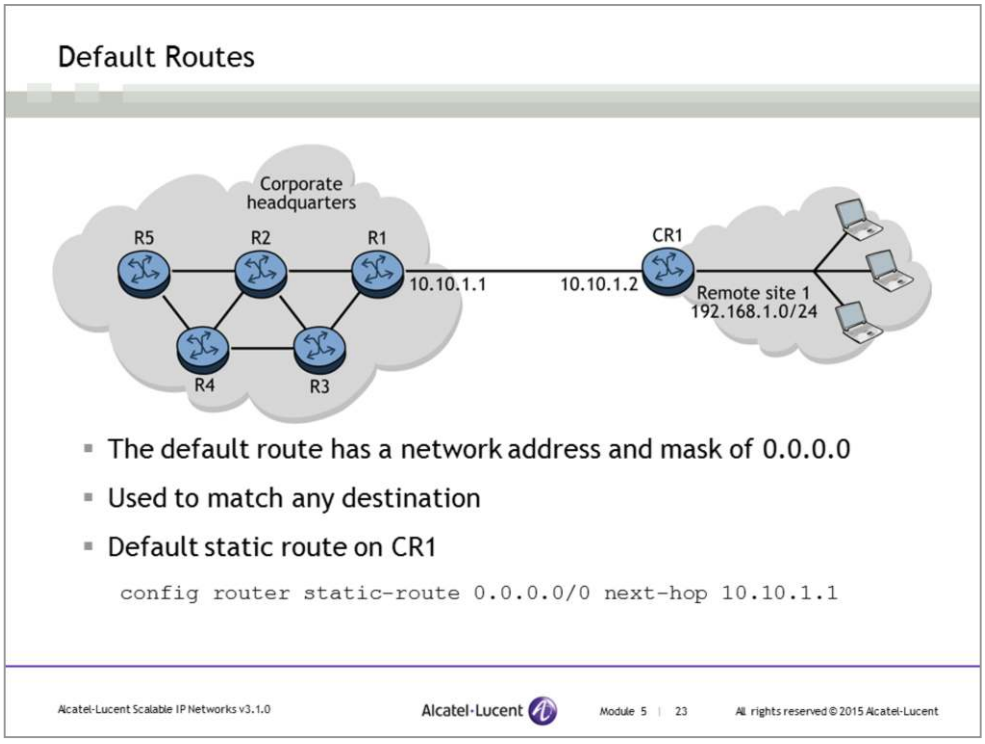
In this example, the corporate headquarters network is connected to two remote sites. The corporate site provides the remote sites with resources and Internet access. Because there is only one link connected between the corporate network and each of the remote sites, the corporate site will only send traffic to its remote sites through that link. A remote network like this, with only one connection to the backbone network, is often referred to as a *stub network*.

For any two routers to forward data to each other bidirectionally, a static route needs to be configured on both routers.

By configuring a static route on router R1, traffic destined for network 192.168.1.0/24 will exit out of the interface on R1 to CR1. A static route configured on router R5 will send traffic to CR2. If router R2 or any of the other corporate routers want to reach either remote site, they must also be configured with a static route in the correct direction. For traffic to flow in both directions, the remote networks must also be configured with static routes to reach the corporate network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



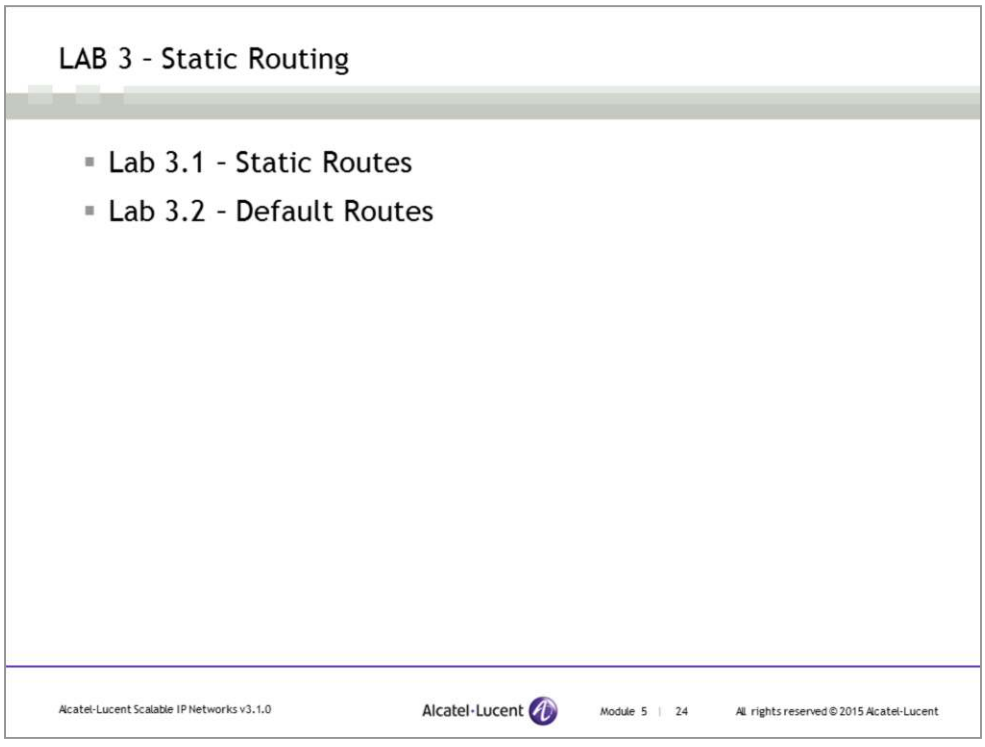
A static default route in the routing table is a wildcard entry that fits any destination. The route is used when the destination address of a packet does not match any other entry in the routing table. A default route is often used on a stub network when there is only one path to reach the other remote networks. The default route has a network address and mask of 0.0.0.0.

It would be cumbersome to configure a large number of static routes on CR1 for each network that is reachable through its single link to corporate headquarters. It would also be unnecessary since all routes would point to the same next hop. It would be very useful in this case to have a way to simply specify that “all” routes are reachable through a static route to a certain next hop. This functionality is achieved through the use of a default route.

In this slide, for Remote site 1 to access the resources of the corporate network, it does not need to list every entry in its routing table for every resource that it needs to send traffic to. Therefore, it uses the default route to match any possible route. The default route is the longest match in the routing table when nothing else matches.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

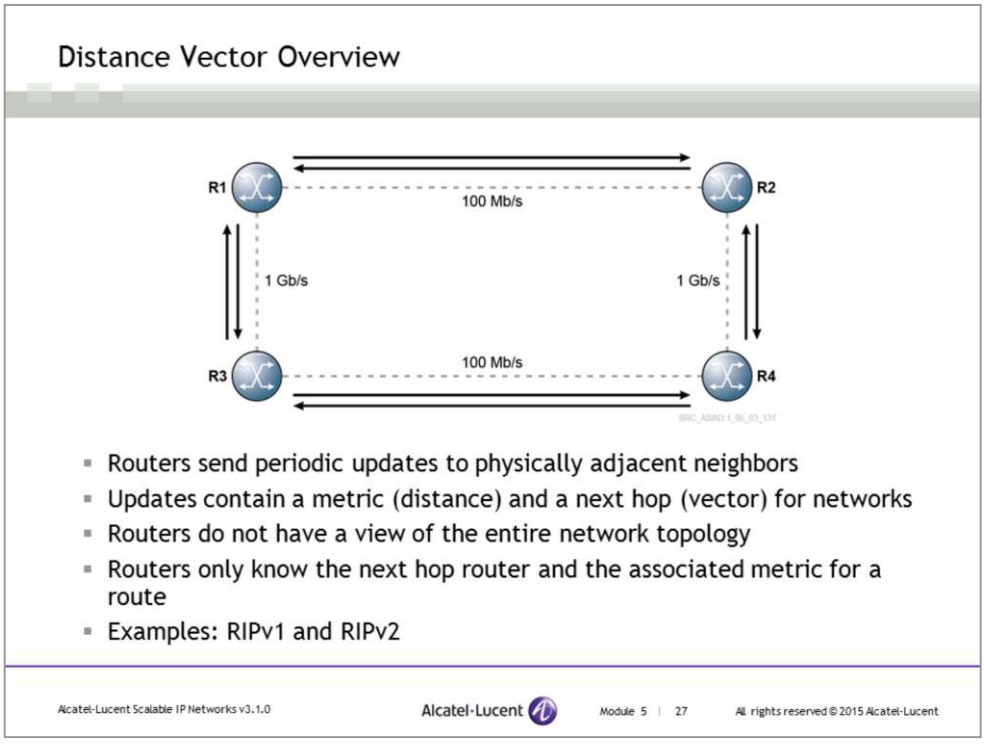
After successful completion of this section, you will be able to:

- Describe the basic operations of distance vector protocol
- Describe the basic operations of link state protocol
- Compare the differences between distance vector protocol and link state protocol

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 26 All rights reserved © 2015 Alcatel-Lucent



With a distance vector routing algorithm (sometimes referred to as Bellman-Ford, after the original algorithm designers), a router periodically passes a copy of its routing table to all its neighbors. These regular updates between routers communicate topology changes because each router is continually receiving a current copy of the entire routing table from its neighbor. Each router is aware of a metric (distance) to particular route and its next hop (vector). Note that the router does not have a picture of the topology. The router simply knows the next router that it sends packets to for a given destination and the associated metric for that route.

Each router receives a routing table from its direct neighbor.

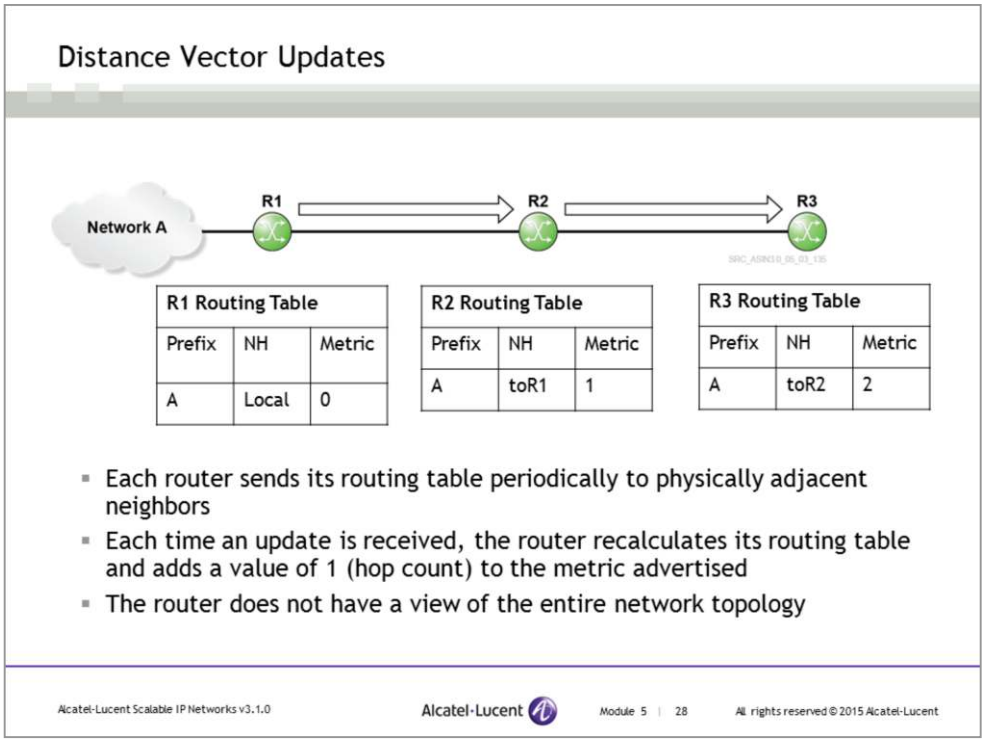
- In this slide, R2 receives a routing update from R1.
- R2 uses the information received from R1 to recalculate its routing table.
- R2 then sends its routing table to R4.
- This step-by-step process occurs in all directions between direct neighbors.

IMPORTANT — With distance vector, a routing table is not transmitted beyond the immediate neighbor. For example, R4 does not receive a routing update directly from R1. R4 receives the routing updates only from its directly-connected neighbors, so R4 is only aware of R1's routes via R2 and R3.

The distance vector algorithm allows network metrics to accumulate. Each router maintains a routing table with the next hop for all of the listed destinations.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



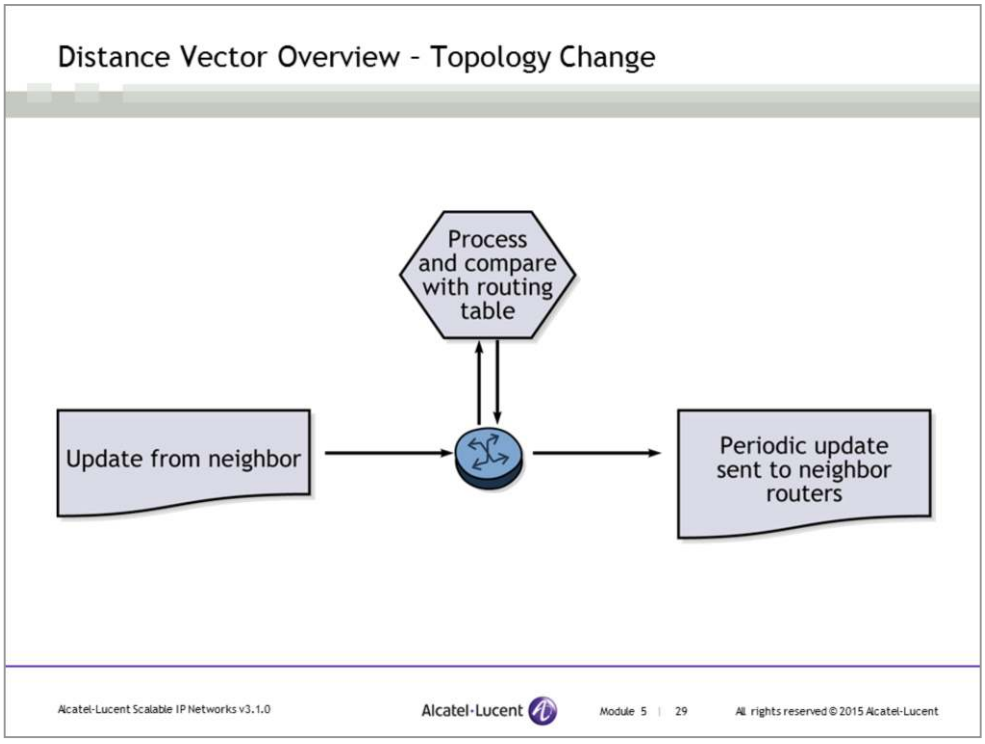
In this slide, router R1 learns about a new locally connected network, network A. Periodically, router R1 will send its routing table to its adjacent neighbor, R2. When R2 receives the routing table update from R1, R2 installs the update in its routing table and adds the value 1 to the metric advertised by R1. In this case, the network A will be installed in R2's routing table with a metric of 1 (1+0).

Periodically, router R2 will also send its routing table to its adjacent neighbor, R3. When R3 receives the routing table update from R2, R3 installs the update in its routing table and adds the value 1 to the metric advertised by R2. In this case, the network A will be installed in R3's routing table with a metric of 2 (1+1).

With distance vector protocol, the router does not have a view of the entire network topology. For example, R3 only knows that Network A can be reached through the next hop router, R2 with a metric of 2. R3 does not know where Network A is located.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

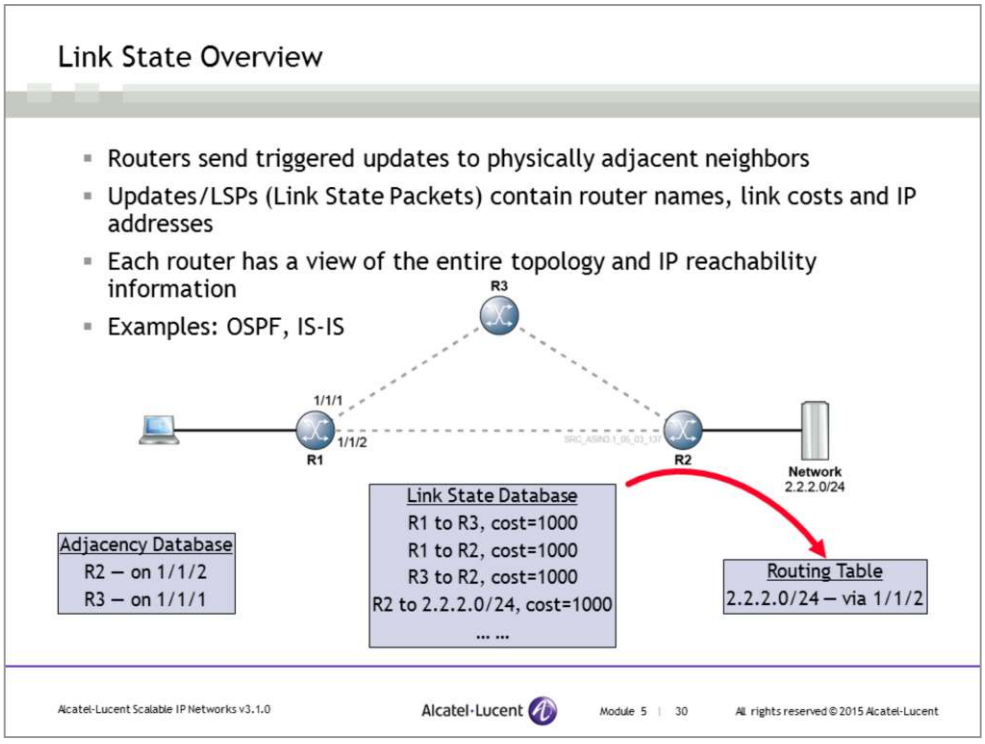


This slide shows the distance vector step-by-step process for updating all routers in a network when a topology change occurs.

- Each router sends its entire routing table to each of its adjacent neighbors. This table includes reachable addresses, a value that represents the distance metric, and the IP address of the first router on the path to each network that the router knows about.
- As each router receives an update from its neighbor, the router calculates a new routing table and transmits the table to each of its neighbors at the next interval (distance vector routing updates occur at regularly-timed intervals).
- In a very large network with many routers, it can take a long time for all the routers in the network to learn about a topology change. Therefore, distance vector protocols have a high convergence time, which is very undesirable.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Link-state routing protocols maintain a complete database of topology information. While distance vector protocols have nonspecific information about distant networks, link-state routing protocols maintain full knowledge of distant routers and how they interconnect. The link-state routing protocols have a view of the entire network topology.

Link-state protocols function by flooding link state packets (LSPs) throughout the network. LSPs are used to transmit the information required to build the topological database, which is used by the Shortest Path First (SPF) algorithm to build an SPF tree. An SPF tree is simply a view of all the routes in the network and the shortest path needed to reach them. Using the SPF tree, link-state protocols build a routing table of paths to each network destination. When a link-state topology changes, all routers must become aware of the change so they can update their routing tables accordingly. This involves propagating common routing information to all routers in the network. To achieve information convergence, each router performs the following:

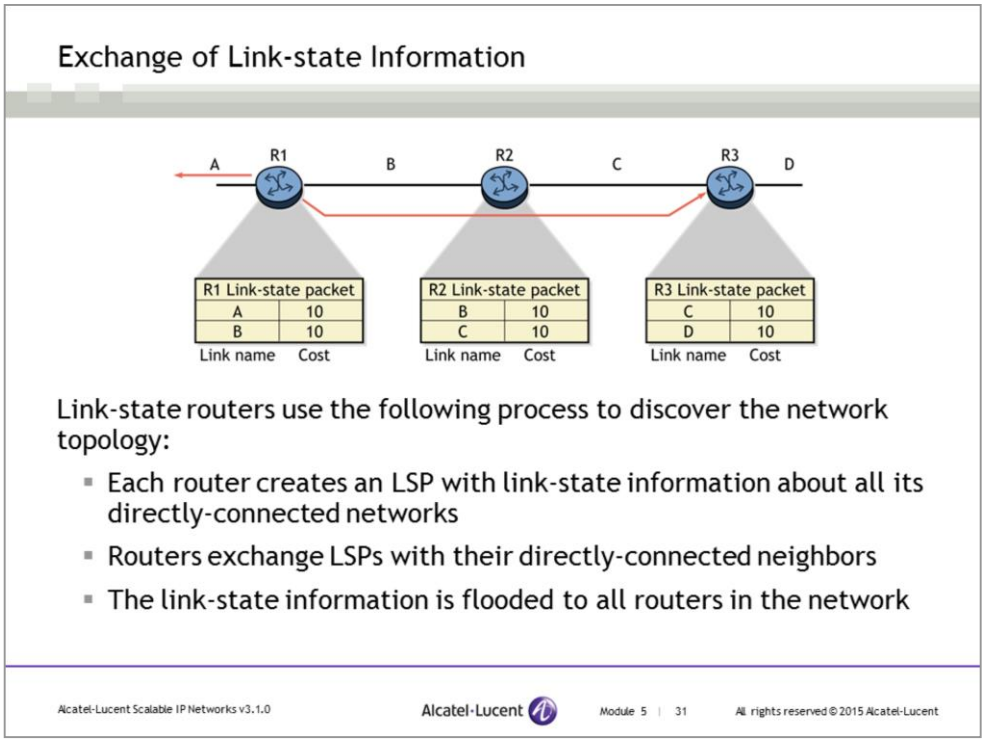
- Keeps track of it neighbors
- Builds an LSP that lists neighbor router names and link metrics (cost). This includes new neighbors, changed metrics, and links to neighbors that are down.
- Sends out the LSP so that all routers receive the LSP
- Upon receiving an LSP, records the LSP in its database so that it has the most up-to-date topology information
- Using accumulated LSP data, builds a complete network topology, and independently executes the SPF algorithm to calculate routes to every network
- Each time there is a change to the link-state database, the router recalculates the best paths and updates the routing table

Link state protocols keep three databases in the router:

- The *adjacency database*, sometimes called the neighbor database, keeps track of all of the other routers that are directly attached. The adjacency database is maintained with periodic hello messages.
- The *link state database* (LSDB) stores the most recent LSPs sent by all the routers in the network. The database is used to create the SPF tree that ultimately creates the routing table.
- The *routing table*, sometimes called the forwarding database, is used by the router to optimally forward IP packets to the destination network.

 All rights reserved © 2015 Alcatel-Lucent

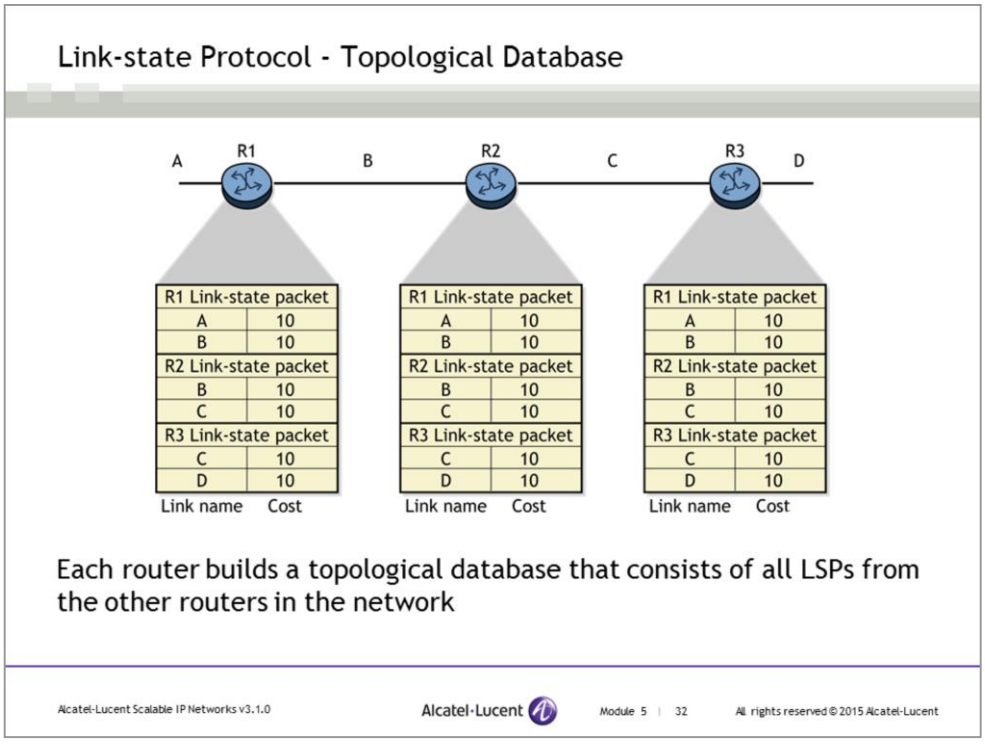
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When link-state protocols are used, each router keeps a database of each of its links and the associated cost for each link. The cost is usually based on a default value that is a function of the speed of the interface.

 All rights reserved © 2015 Alcatel-Lucent

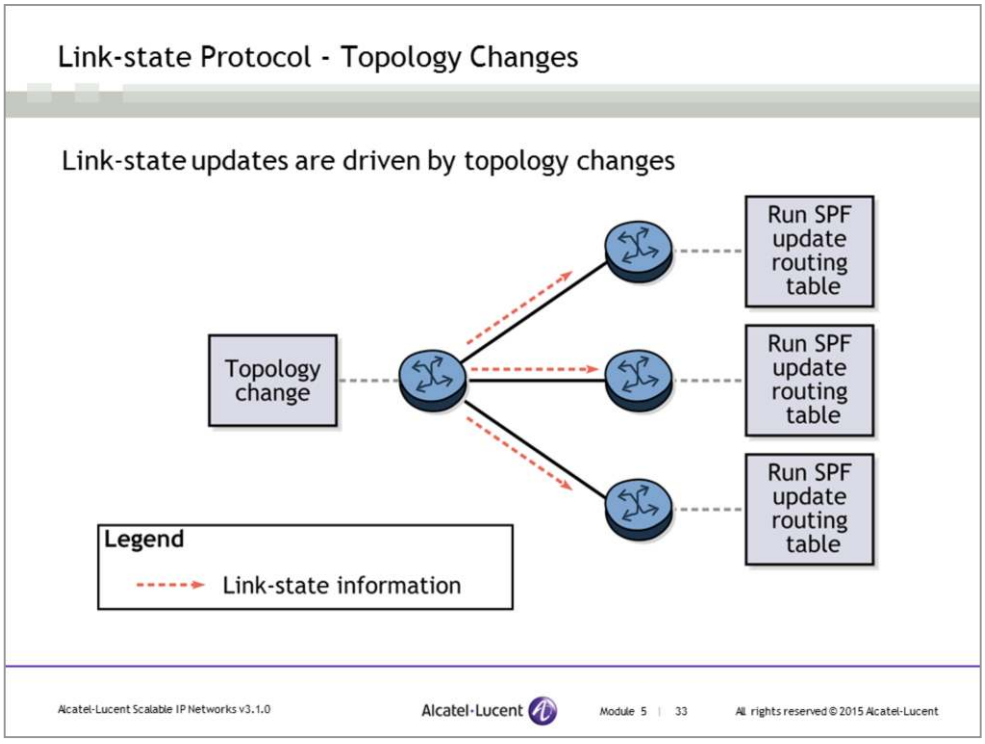
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Once routers update each other with their LSPs, the router records the LSPs in the database so that it has the most up-to-date topology information. Each router will maintain a link-state database that contains all the information for all links in the network. Each router should share a common view of the links in the network because each LSP is flooded to every router. Using accumulated LSP data, a router builds a complete network topology and independently executes the Shortest Path First (SPF) algorithm to calculate routes to every network. Each time there is a change to the link-state database owing to a link state update, the router recalculates the best paths and updates the routing table accordingly.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



When a router recognizes a topology change (that is, link down, neighbor down, new link, or new neighbor), the router must notify its neighbors of this change. To do this, each link-state router performs the following:

- The router that recognizes the change sends new link-state information about the change by flooding it throughout the network.
- When a router receives new link-state information, the router must update its topological database and send the information to its neighbors.
- The SPF algorithm must be run against the new topological database to update the routing table with the new information.

Each time that there is a topology change that causes an update to the topological database, the SPF algorithm must be run. At the end of this process, every router possesses a common view of the entire network and has received information directly from other routers in order to independently build its topological view. This contrasts with the view of a router running a distance vector protocol, in which each router has only a limited amount of information about the network that it receives from its neighboring router.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Distance Vector vs Link State

Distance vector	Link state
Views the network topology from the neighbor's perspective	Gets a common view of the entire network topology
Adds distance vectors from router to router	Uses SPF algorithm to calculate the best path to other routers
Updates the metric value for the route received with a hop count of 1	Does not update the metric value for the route update received
Frequent periodic updates	Event-triggered updates
Slow convergence	Faster convergence
Passes copies of the routing table to neighbor routers	Passes link-state routing updates to other routers

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 34
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

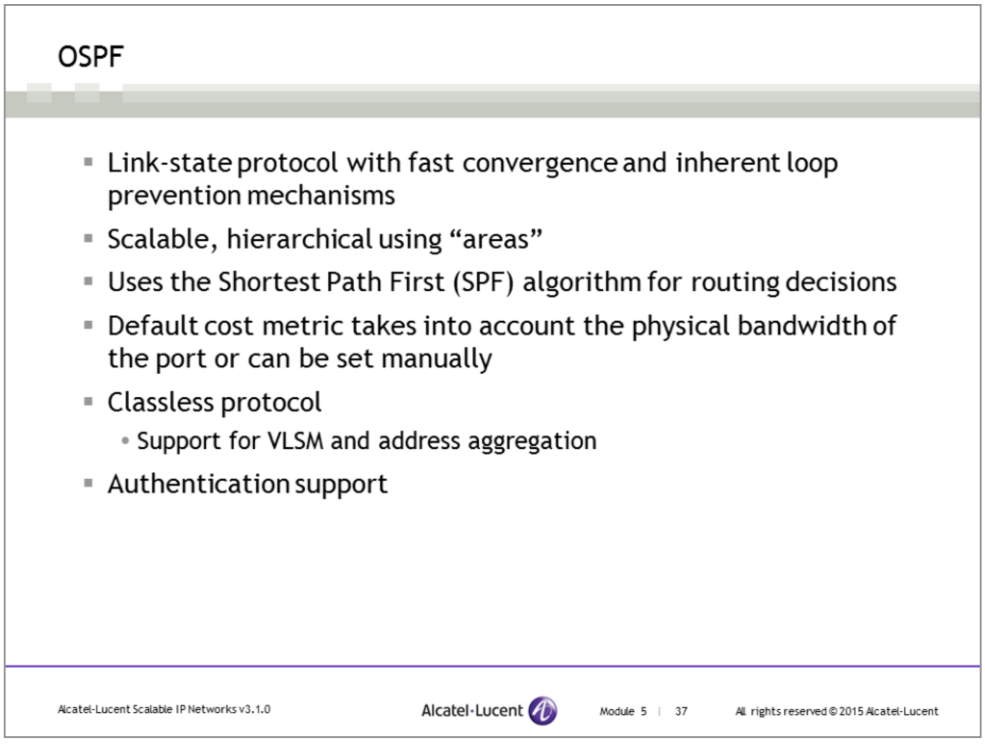
After successful completion of this section, you will be able to:

- Describe the characteristics of OSPF
- Explain the functions of router ID
- Describe the process of forming an OSPF point-to-point neighbor adjacency
- Describe how OSPF floods link-state information and ensures topological database synchronization
- Explain how OSPF metric is calculated
- Use the CLI to configure OSPF and show OSPF configuration

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 36
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



OSPF is a link-state routing protocol. As such, it uses the SPF algorithm to find the shortest path to every destination in the network. Link-state routing protocols are inherently loop free and have a fast convergence time. Link-state routing protocols have limited scalability, so OSPF supports hierarchy with the concept of areas. This greatly increases the scalability of OSPF.

The subnet mask is carried in OSPF link-state updates, so variable length and noncontiguous subnets are supported. Route aggregation is also supported to enable more efficient address management. OSPF supports authentication for security.

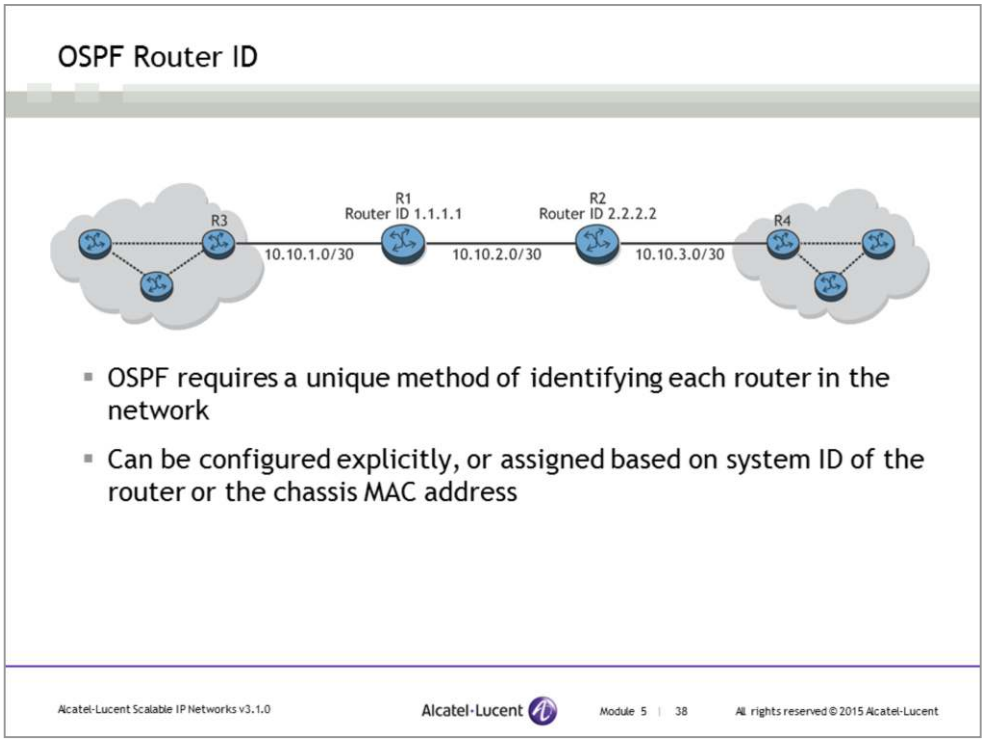
The OSPF cost metric is based on the physical bandwidth of the port. This allows OSPF to make its path decisions based on the path that has the most bandwidth rather than the least number of hops.

The traffic engineering extensions to OSPF allow the protocol to track and advertise the available bandwidth, administration groups, maximum number of hops, and so on. This feature is used by MPLS to create traffic tunnels and is covered in the Alcatel-Lucent MPLS course.

OSPF Version 2 (RFC 2328) is a widely-deployed, well-known protocol for IPv4. OSPF Version 3 (RFC 5340) is standardized and supports IPv6.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



OSPF uses a router ID to uniquely identify a router. The router ID is a 32-bit number assigned to each router running OSPF. Routers running OSPF use the router ID of neighboring routers to establish adjacencies and to flood Link State Advertisements (LSAs).

The router ID that is used for OSPF can be configured explicitly using the following command: `configure router router-id <ip-address>`. This router ID is also used for other routing protocols, such as BGP.

To use a separate router ID for different protocols, you can override this high-level router ID with an OSPF-specific router ID using the following command: `configure router ospf router-id <ip-address>`.

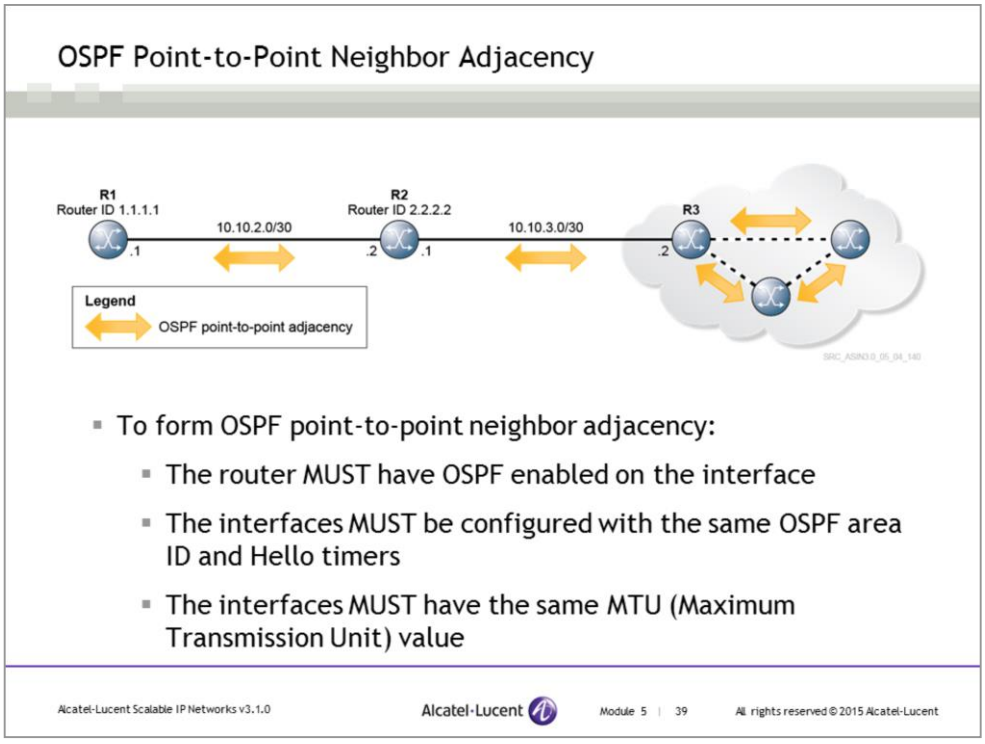
If a router ID is not configured but a system interface is configured with an IP address, the system IP address is used as the OSPF router ID. To configure a system interface, use the following command: `configure router interface system address <ip-address>/32`.

If neither a router ID nor a system interface address is configured, the last four octets of the chassis MAC address are used as the OSPF router ID. The chassis MAC address can be viewed using the following command: `show chassis`.

The OSPF router ID selection is not pre-emptive. If the OSPF router ID is reconfigured, the change will not take effect until the OSPF routing process is restarted.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



OSPF is a dynamic routing protocol that is based on routers exchanging link-state information with each other.

Two OSPF routers must create an OSPF neighbor adjacency before they can exchange routing information.

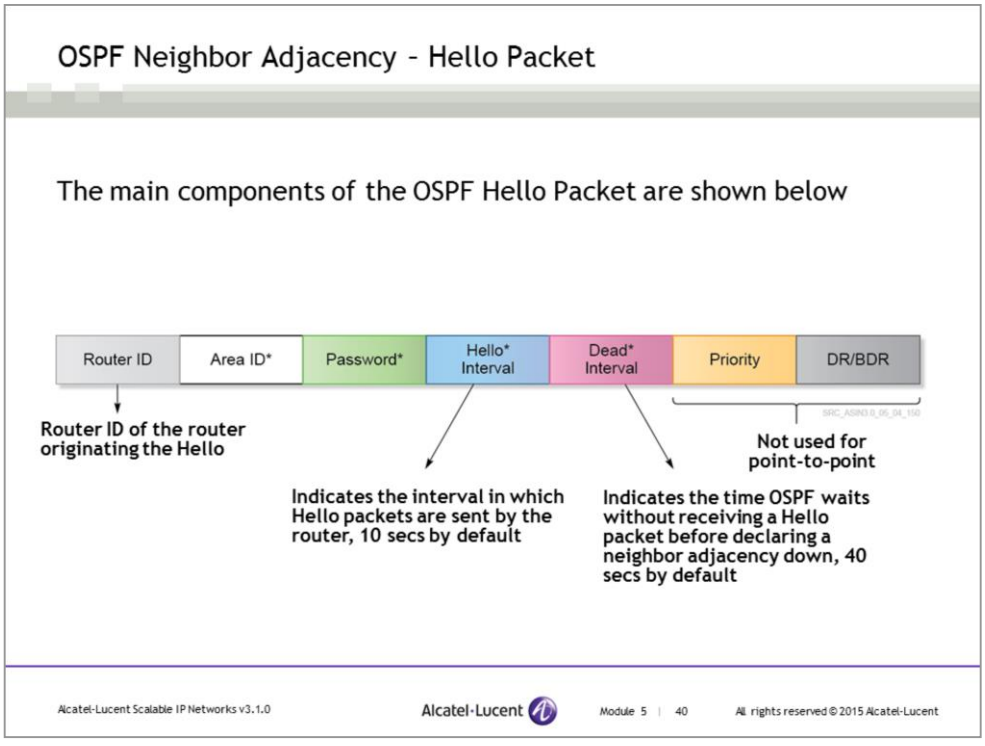
On point-to-point OSPF networks, neighboring routers become fully adjacent with each other once they detect each other via OSPF hello packets. For example, in this slide, router R2 becomes fully adjacent with both routers R1 and R3. All neighbor adjacencies in the point-to-point network are indicated with the arrows. For OSPF routers on a point-to-point network to become adjacent, the routers must have OSPF enabled on the interface and must be configured with the same area ID and Hello timers.

Routers can also be connected on a shared broadcast segment, such as Ethernet, rather than a point-to-point segment. On a broadcast segment, additional steps are performed to reduce the amount of OSPF control traffic that flows between routers on the segment. This involves electing designated routers (DRs) and backup designated routers (BDRs) to handle adjacency formation. However, these concepts are beyond the scope of this course and are covered in the Alcatel-Lucent Interior Routing Protocols course. This course discusses only the point-to-point scenario.

Note that the default OSPF interface type is broadcast for Ethernet interfaces and must be explicitly configured as point-to-point. The configuration will be presented later in this section.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Parameters that are denoted with an asterisk must be set the same on both routers to form an adjacency or to keep an adjacency alive. These parameters are:

Area ID – Used for OSPF hierarchy; it must be configured even if there is only a single area. It must be the same on all adjacent routers.

Password – Used only for OSPF authentication

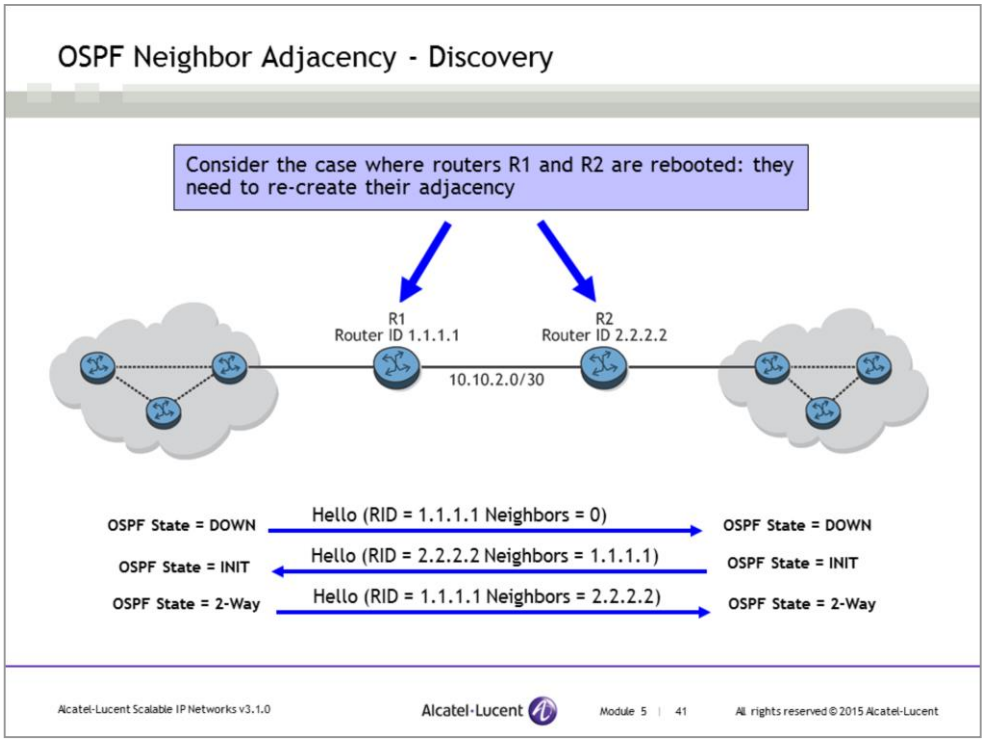
Hello Interval – The interval at which hello packets are sent; defaults to 10 seconds

Dead Interval – The time OSPF waits without receiving a hello packet to mark a neighbor down; defaults to 40 seconds

Hello packets are sent between routers to form an adjacency and to proceed to an exchange of link state tables. They are also used as a keep-alive after the adjacency is formed. On point-to-point links, OSPF traffic is always sent to the reserved multicast address 224.0.0.5.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



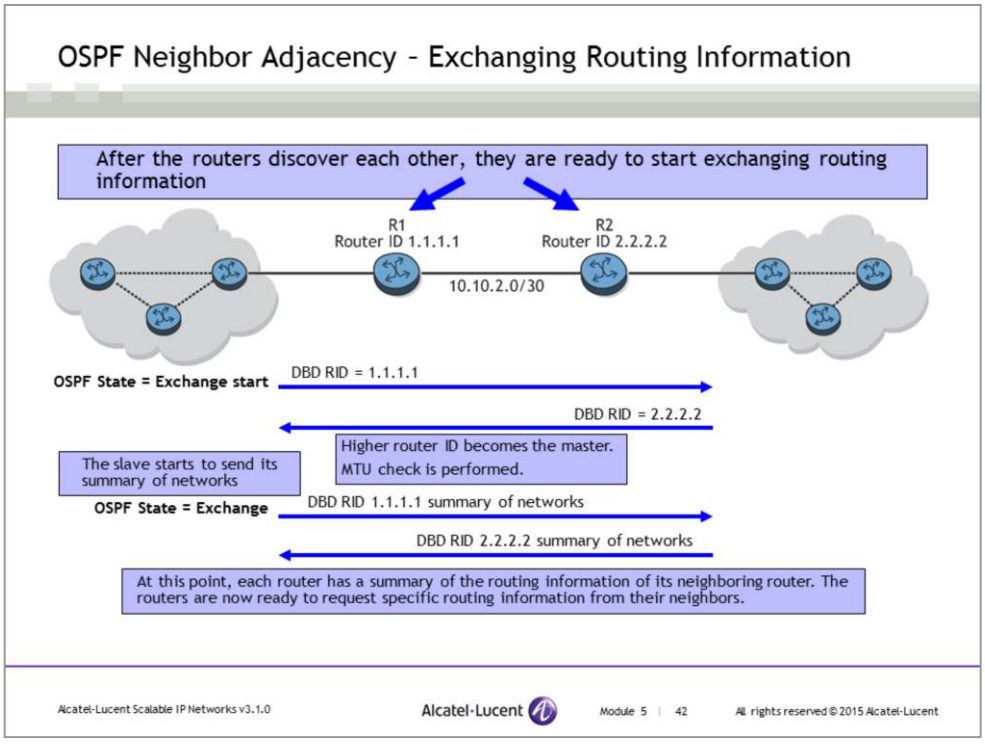
Hello messages are used at the beginning of the process of forming an adjacency. In this slide, routers R1 and R2 have been rebooted and therefore need to form a new adjacency.

The process of forming an adjacency has several distinct stages:

- When both routers are first powered up, they are in the OSPF **down** state.
- Both OSPF routers send OSPF hello packets to discover each other and proceed to the **init** state.
- When the discovery process is complete, the routers are in a **2-way** state and are ready to exchange routing information.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In the Exchange Start (ExStart) state, both routers send database description (DBD) packets and establish a master-slave relationship. The DBD packet is used to describe the content of the topological database; multiple packets may be used to describe the database. One of the routers is the master, the other is the slave. The router with the highest router ID becomes the master (R2 is the master and R1 is the slave in this example). The determination of when to send a DBD packet depends on whether the router is master or slave. The master sends DBD packets, which are acknowledged by the DBD packets sent by the slave.

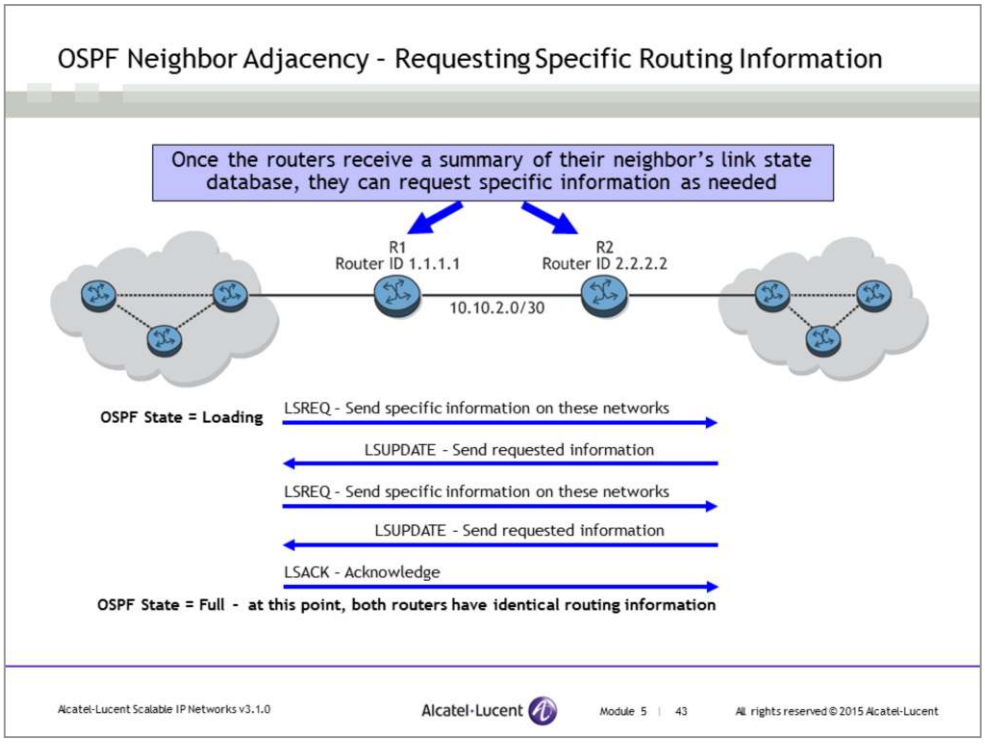
Once the master-slave relationship is established during the exchange start state, the DBD is sent by the slave router to the master router to provide a summary of the networks that the slave router knows about. The master router then sends the slave router a summary of the networks that the master router knows about.

After the master and slave routers exchange their summary information, the exchange state is complete. Now the router determines which routing information it misses and which of the neighbor's routing information is more recent.

Maximum Transmission Unit (MTU) checking is also performed in the exchange start state. The OSPF MTU from both neighbors must match to proceed beyond the exchange start state. The OSPF MTU can be configured explicitly on the OSPF interface. If the MTU is not configured, the physical port MTU becomes the OSPF MTU. Therefore, if an OSPF MTU is not configured, the physical port MTUs must match to create an adjacency. The OSPF MTU determines the maximum size of the OSPF control packets, which is typically the size of the link-state update and link-state request packets.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



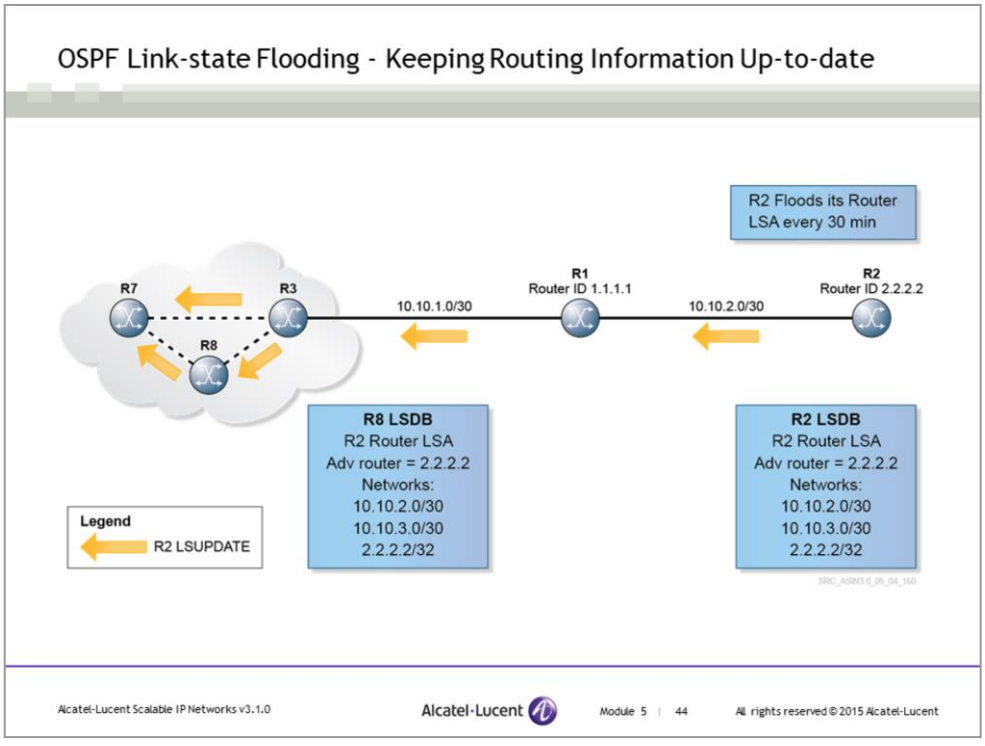
After the exchange state is completed, the routers now proceed to the loading state. Recall that database description (DBD) contains a summary of networks. Based on the information from the database description (DBD) packets, the router sends a Link State Request (LSReq) packet to request specific routing information that it does not have or has older versions of. The neighbor then sends the requested information using Link State Update packets. A link-state update packet contains one or more link state advertisements (LSAs). The LSA is used to describe the routing information. All link-state update packets are acknowledged.

In the Loading state, both routers go through a Request, Reply, Acknowledge sequence until each router has a full view of its neighbor's routing information. At this point, both routers have identical link-state databases and are considered fully adjacent. Once the link-state database is fully up-to-date, each router runs the SPF algorithm to calculate the best path to each destination in the network and uses this information to build its routing table.

In a single area point-to-point network, only the router LSAs (Type 1 LSAs) will be used. In more complex topologies, there are other types of LSAs exchanged.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

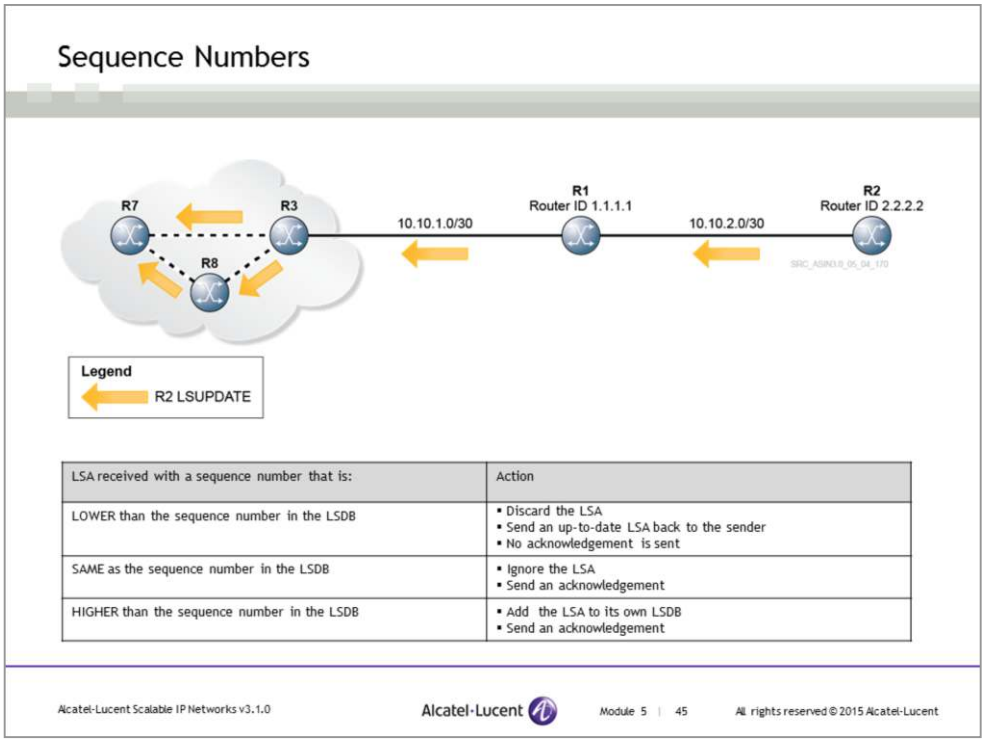


A router LSA, packaged within a link-state update packet, is flooded to all routers in the same OSPF area every time there is a topology change on one of the directly-connected links on the router. If there are no topology changes, the router will still flood the router LSA every 30 minutes. Every LSA has a maximum age of 60 minutes. An OSPF router will age all LSAs in its link-state database and will purge any LSAs for which it has not received a refresh in the last 60 minutes.

Router LSAs on point-to-point networks are always flooded to multicast IP address 224.0.0.5. This is the same multicast address that is used for OSPF hello packets while creating and maintaining an OSPF neighbor adjacency.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



OSPF uses a sequence number to ensure that LSAs are not transmitted around the OSPF area indefinitely. The acknowledgement of LSAs is used to guarantee the reliability of LSA transmission to neighboring routers.

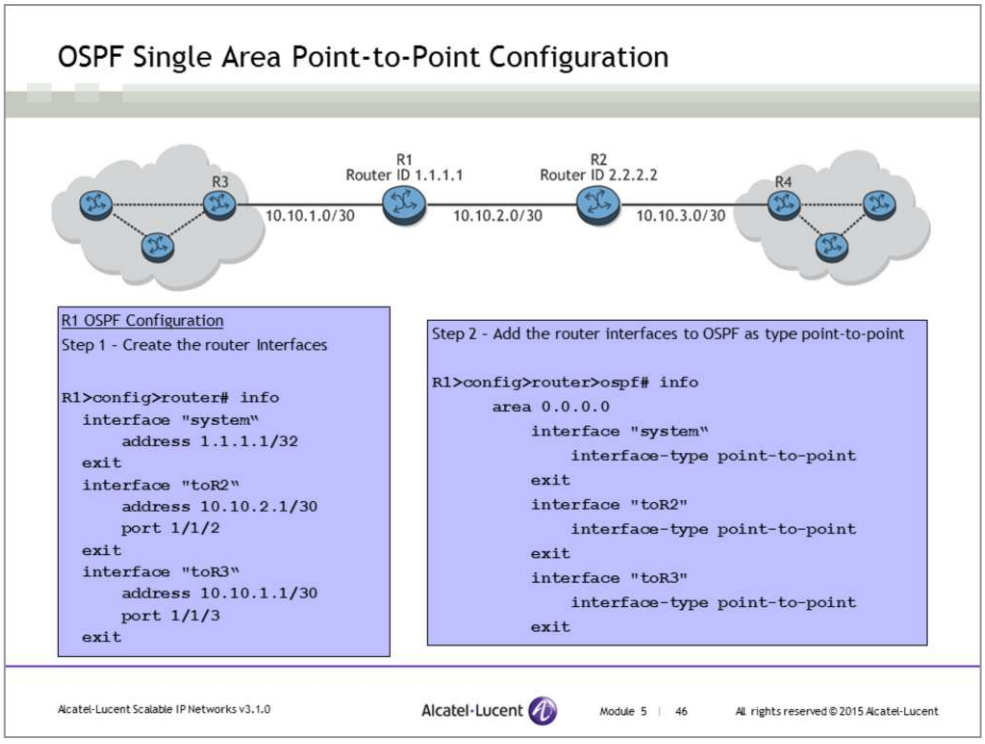
The following rules are applied by the OSPF router to process the LSAs that are received from its neighbors.

- If the sequence number is lower than the sequence number in the link-state database, the incoming link-state information is considered to be out of date and is discarded. The receiving router will update the sending router with an up-to-date LSA from its own database.
- If the sequence number is the same as the number in the database, an acknowledgement is sent. The incoming link-state information is then discarded.
- If the sequence number is higher than the number in the database, the new link-state information is added to the link-state database, an acknowledgement is sent and the link-state information is forwarded to its neighbors.

The protocol field in the IP header identifies the service in the next higher level in the protocol stack to which data is passed. All OSPF control packets use the protocol ID 89 in the IP protocol field. OSPF does not use TCP or UDP as a transport layer. Instead, IP uses the protocol ID 89 to extract all OSPF packets for the OSPF process on the router.

All rights reserved © 2015 Alcatel-Lucent

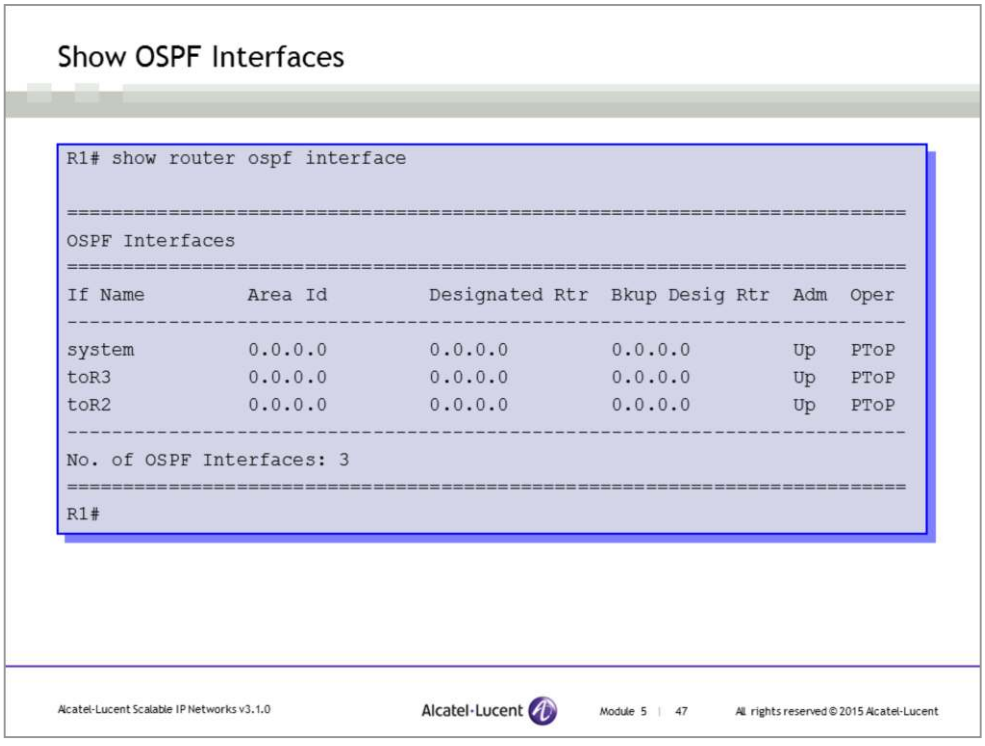
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The steps for OSPF configuration for router R2 and the other routers in the network follow router R1's configuration. The only difference is that you must verify that the IP addresses and port numbers on the interfaces are accurate. It is also good practice to verify that the interface names have the correct descriptions.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



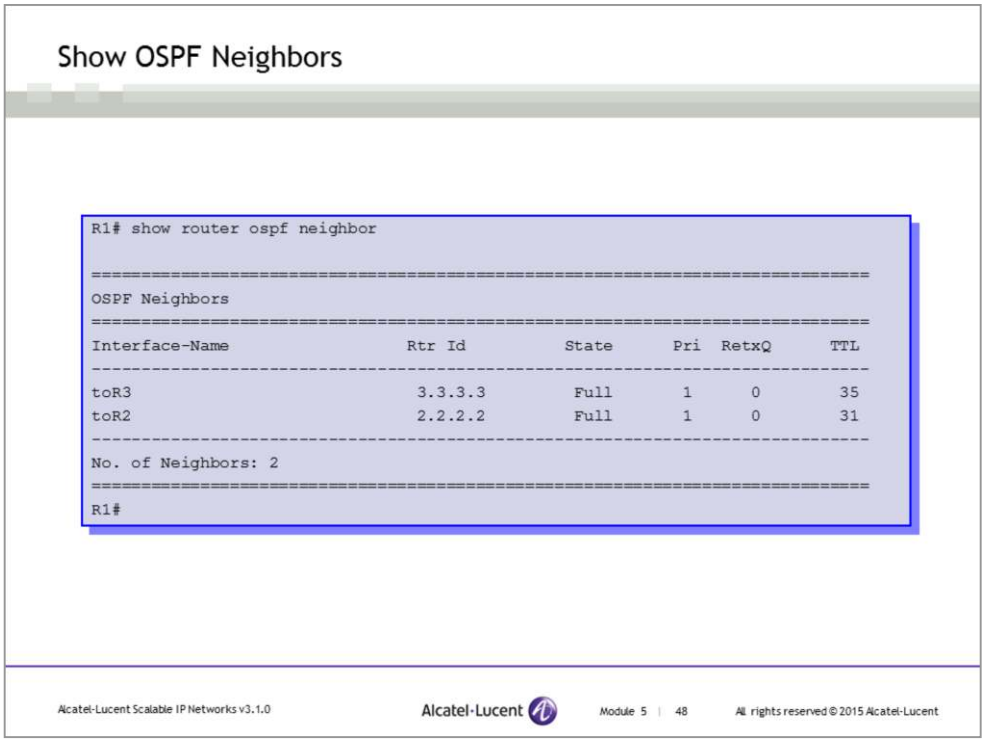
This slide shows the interfaces that are running OSPF, including their names and the areas they belong to.

Note that the operating status for the interfaces to routers R2 and R3 is “PToP” because the routers have been defined as point-to-point interfaces in the OSPF configuration.

The “Designated Rtr” and “Bkup Desig Rtr” fields are only applicable to OSPF broadcast interfaces, which are not covered in this course. For OSPF point-to-point Interfaces, the Designated Rtr and Bkup Desig Rtr values are always “0.0.0.0”.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

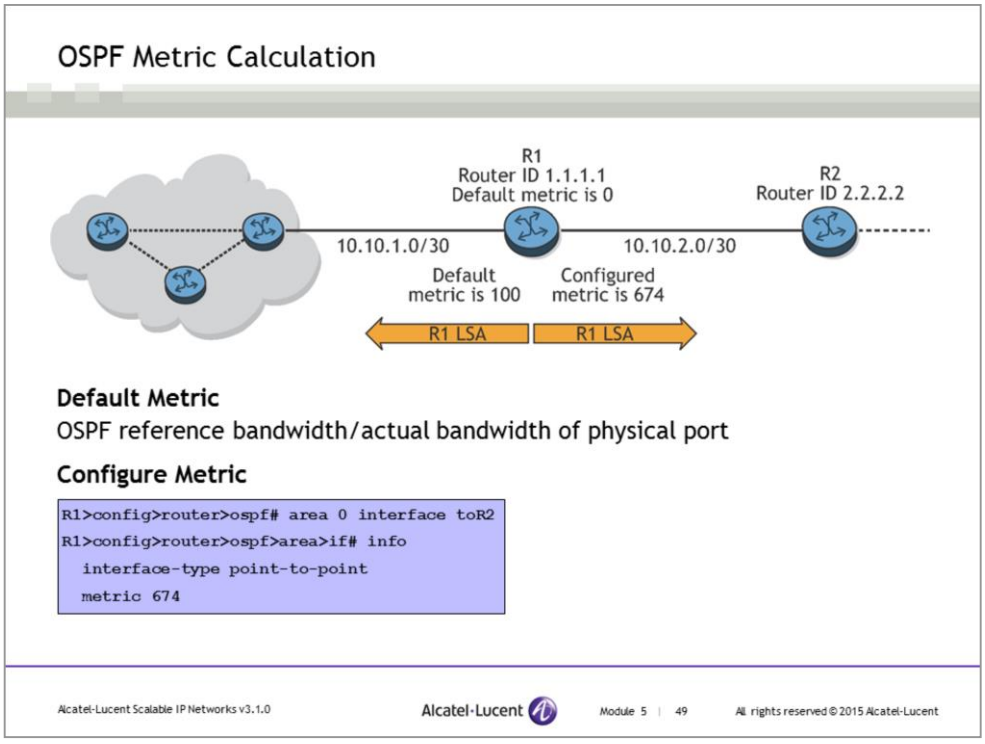


This slide shows the OSPF adjacencies created by router R1 with its directly-connected neighbors. The output includes the logical router interface that the adjacency was created on and the router ID of the neighbor.

The neighbor state is Full when the routers have synchronized their databases and have fully created their adjacency. Other states that may be displayed are: Init, 2Way, Exstart, and Exchange, which are usually only briefly displayed.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The OSPF metric advertised in router R1's LSA for an interface is automatically calculated based on the OSPF reference bandwidth, which is 100 Gb/s by default. The metric is calculated by dividing the reference bandwidth by the actual bandwidth of the link.

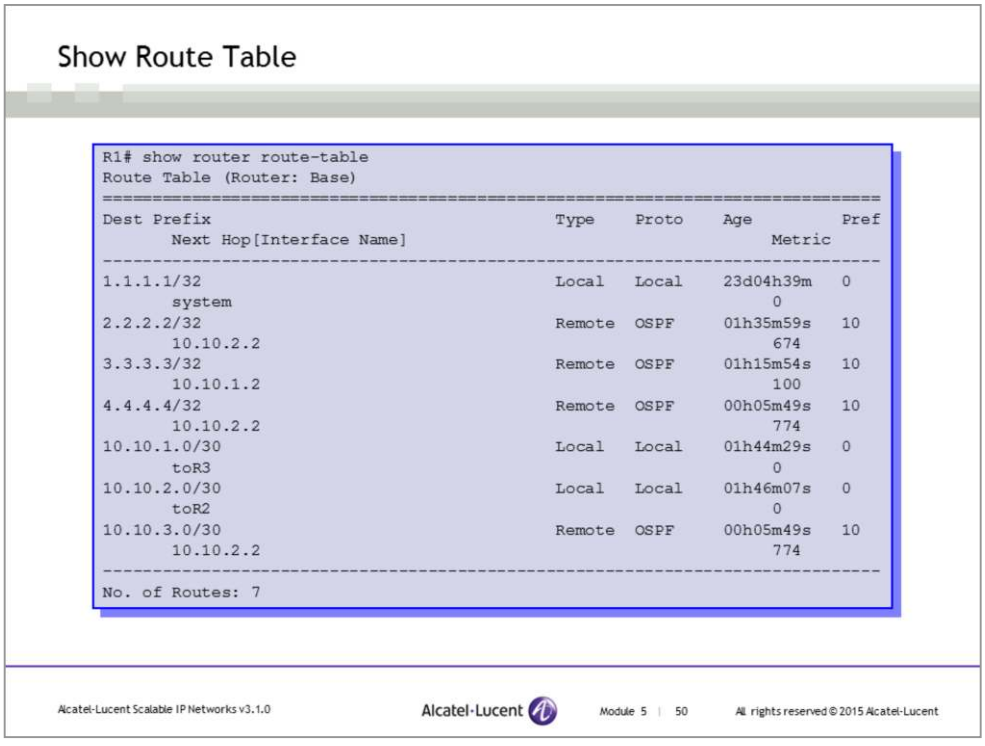
For example, the metric of a 1 Gb link is 100 Gb/s ÷ 1 Gb/s = 100. The metric of a 100 Mb link is 100 Gb/s ÷ 100 Mb/s = 1000. Lower bandwidth links have a higher metric (cost) and are thus less preferred.

Alternatively, the OSPF metric of an interface can be configured in the OSPF interface context.

The default metric of the system and loopback interfaces on a router is zero.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the forwarding information used by the router to forward traffic to its destination. Note that local routes always have a metric of 0 and a preference of 0. Therefore, even if OSPF had learned of paths to these destinations, the paths would not be entered in the forwarding table because the preference value for OSPF is 10.

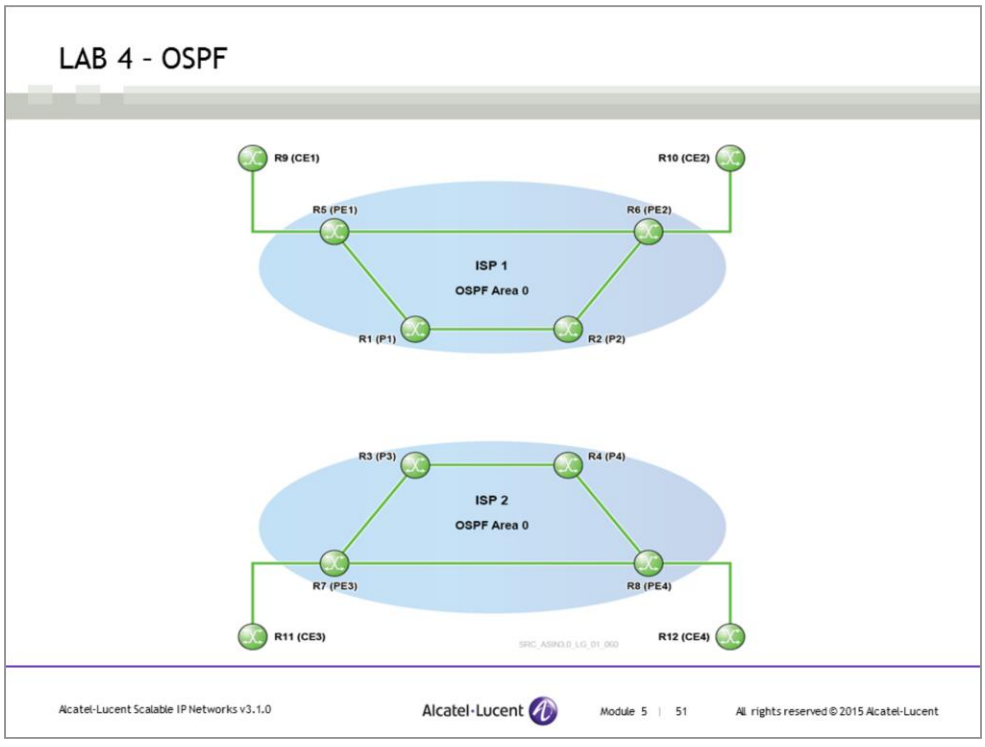
The information also includes the address or name of the next-hop interface. For a local route, the name of the interface is displayed (toR3 or toR2).

For a remotely-learned route, the address of the next hop is displayed (10.10.2.2). A data packet whose destination address matches this entry in the route table will be forwarded to the next hop address.

Since the metric value for the interface toR2 has been changed to 674, the metric for the route originated on router R2 is now 674, instead of the default value of 100.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Section Objectives

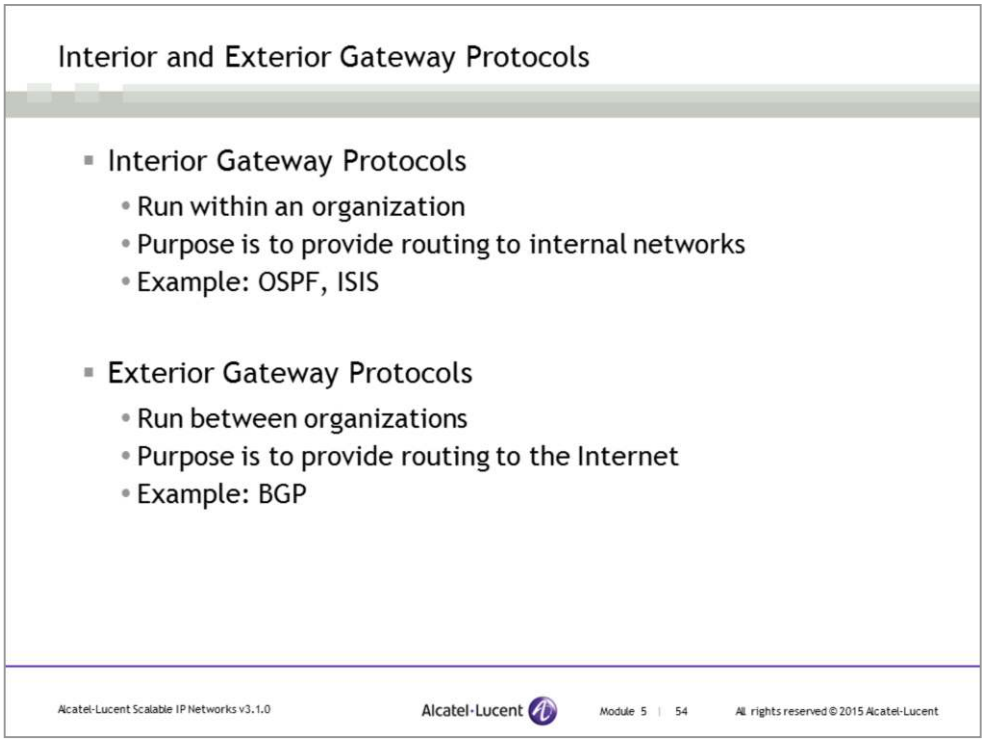
After successful completion of this section, you will be able to:

- Compare the purposes of Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP)
- Define Autonomous Systems in BGP and identify public and private ASs
- Describe the characteristics of BGP
- Compare the differences between iBGP and eBGP
- Describe BGP use cases

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 53
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

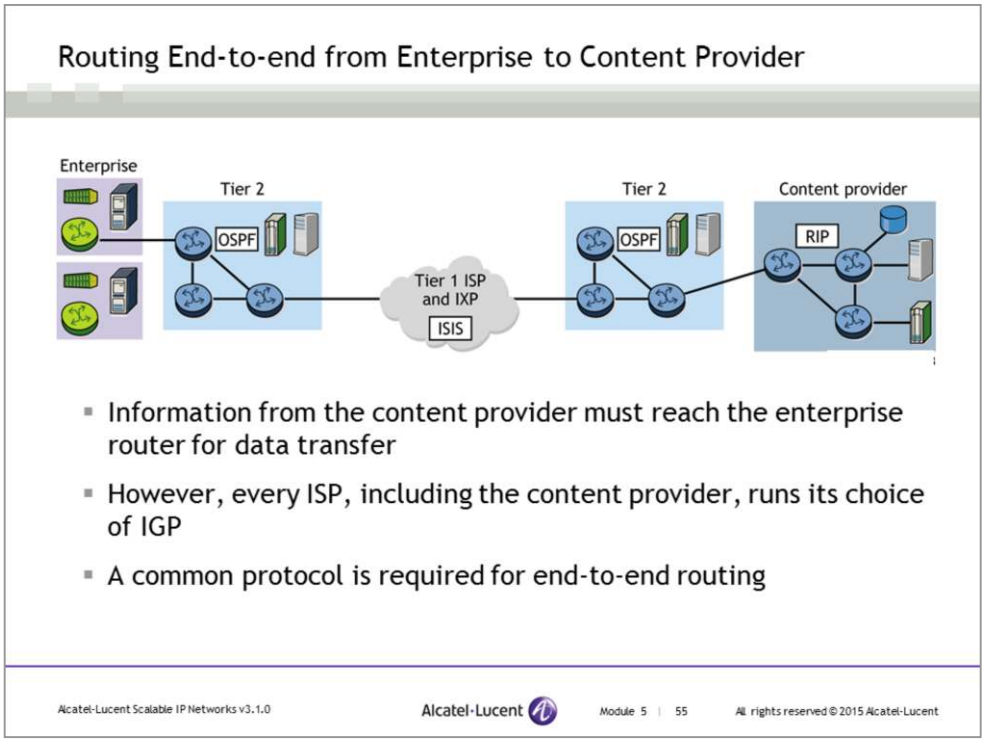


IGP is designed to route between networks within an organization. The networks within an organization are private or public addresses that are typically not advertised to other organizations.

Routing information must also be exchanged between organizations. These routes are public IP addresses because they are exchanged on the Internet. More control is required over the way that traffic flows between organizations - it is not always the shortest path that is preferred. BGPv4 provides many features to control traffic flows between organizations and is the EGP used on the Internet. BGPv4 is also able to scale to very large networks, which is an important requirement in order to manage very large numbers of routes on the Internet.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



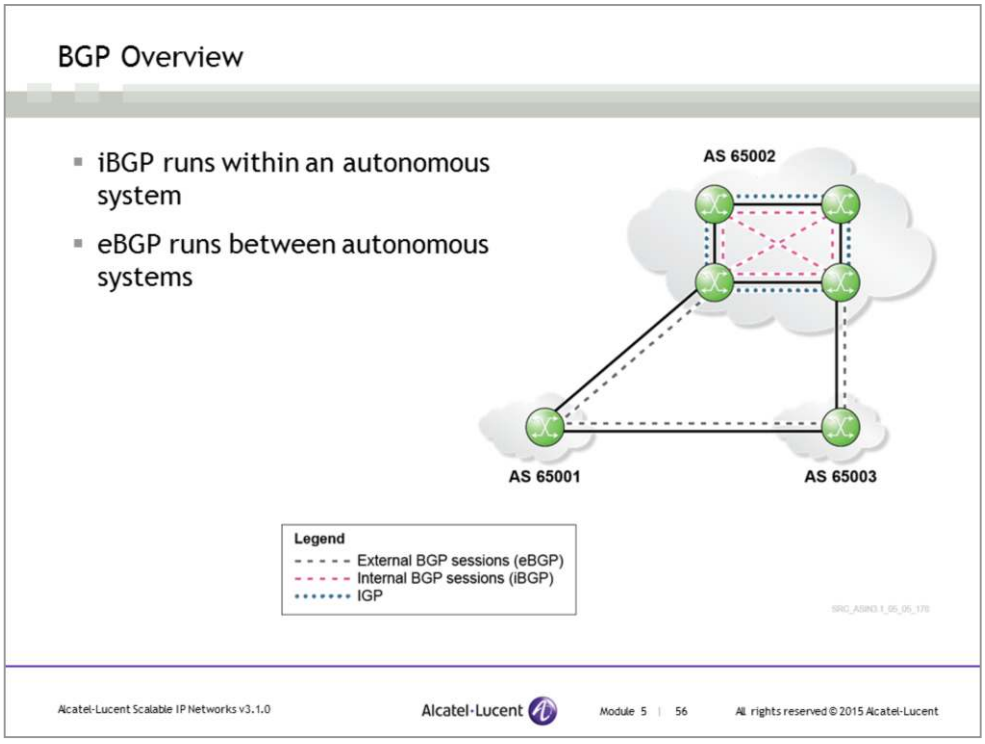
In this slide, the enterprise offices need the address information of the content providers. However, the information from the content provider must traverse many ISPs, and each ISP runs its own choice of IGP. When the origin of the prefix is the content provider that runs OSPF as their IGP and the Tier 1 ISP runs IS-IS, the prefix must be relearned in the Tier 1 ISP as an IS-IS prefix and, therefore, the prefix could lose its original attributes. Every other ISP in the path of the prefix towards the enterprise will need to relearn the prefix in the protocol of its choice. This means that a large number of routing protocol redistributions would have to take place.

In this slide, although end-to-end routing can be achieved by the process of redistribution, there are several disadvantages, such as the following:

- Route redistribution removes the metrics of the original protocol and uses the metrics of the newer protocol. The result is a loss of the “best path” attribute of the route.
- Route redistribution needs to be managed carefully with extensive policies. This is because route redistribution must generally be bi-directional.
- Distributing the Internet addresses into an IGP is not a scalable design. Most routers are not designed to handle the large number of Internet prefixes.
- Route distribution requires a common protocol to run between all routers involved in the transfer of network prefixes from one AS to another.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



From earlier modules of this course, we know that an autonomous system (AS) is a group of networks and networking equipment under a common administration. An IGP (such as OSPF) is used to exchange routing information within the AS, and an EGP (such as BGP) is used to exchange routing information between ASs.

BGP is not a discovery protocol, and BGP routers are not always directly-connected. The only requirements for BGP neighbors is that they can establish a TCP session with each other to exchange routes. The BGP routers that can establish TCP sessions and exchange routes become BGP peers. BGP peers can either be in the same AS or different ASs.

Within an AS, an IGP is required to route traffic between BGP peers so they can establish a TCP session. Between ASs, BGP peers are normally directly-connected, so no IGP is usually necessary to establish those types of sessions.

BGP sessions between routers in different ASs are known as external BGP sessions (eBGP), while sessions between routers in the same AS are internal BGP sessions (iBGP).

BGP is administratively much more complex than an IGP. BGP updates include path information that is used for routing policy enforcement and loop detection between ASs.

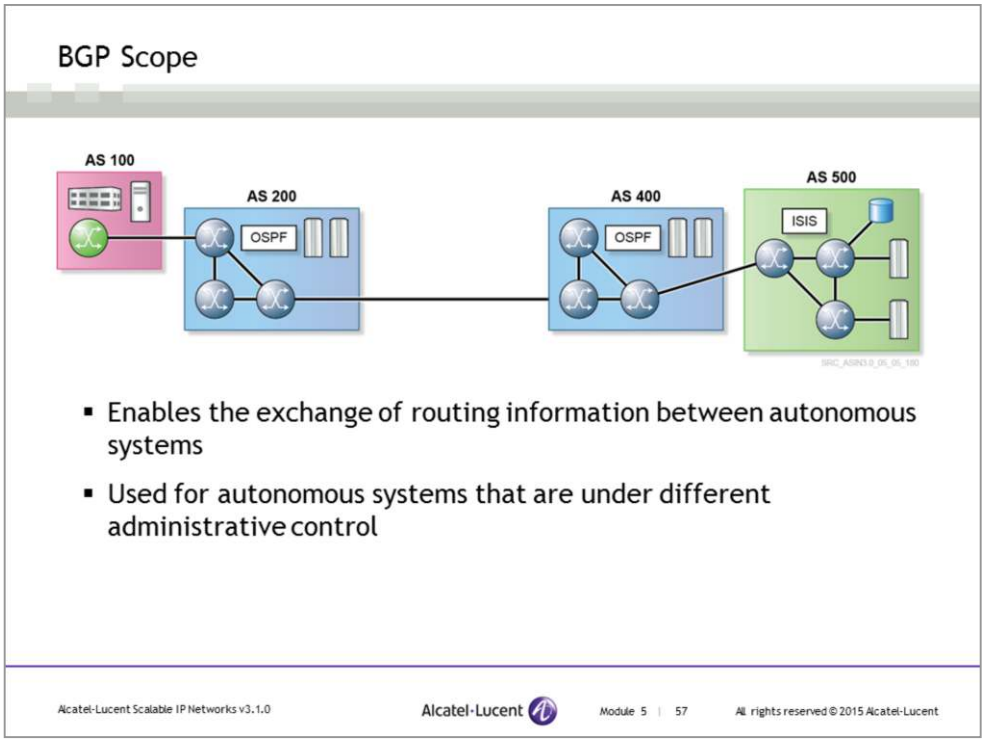
Adding to the complexity of BGP is the fact that topology and routing table sizes become much larger than in an IGP environment. The increased size of the tables means that factors such as CPU loading, memory utilization, update generation, and route processing have greater implications in BGP.

These items, and others, affect convergence. Convergence may be viewed in two ways. *Local convergence* is the time for a router to receive and process all outstanding messages, and achieve a stable topology. *Network convergence* is the time for all routers in the system to achieve a stable topology. In IGP terms, the system is usually the local AS. In BGP terms, the system is the Internet.

Because the entire Internet is the scope of BGP, the administration is more complex than the administration of one AS.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A key strength of BGP is that it enables the implementation of administrative policies to manage traffic flow between autonomous systems based on virtually any policy.

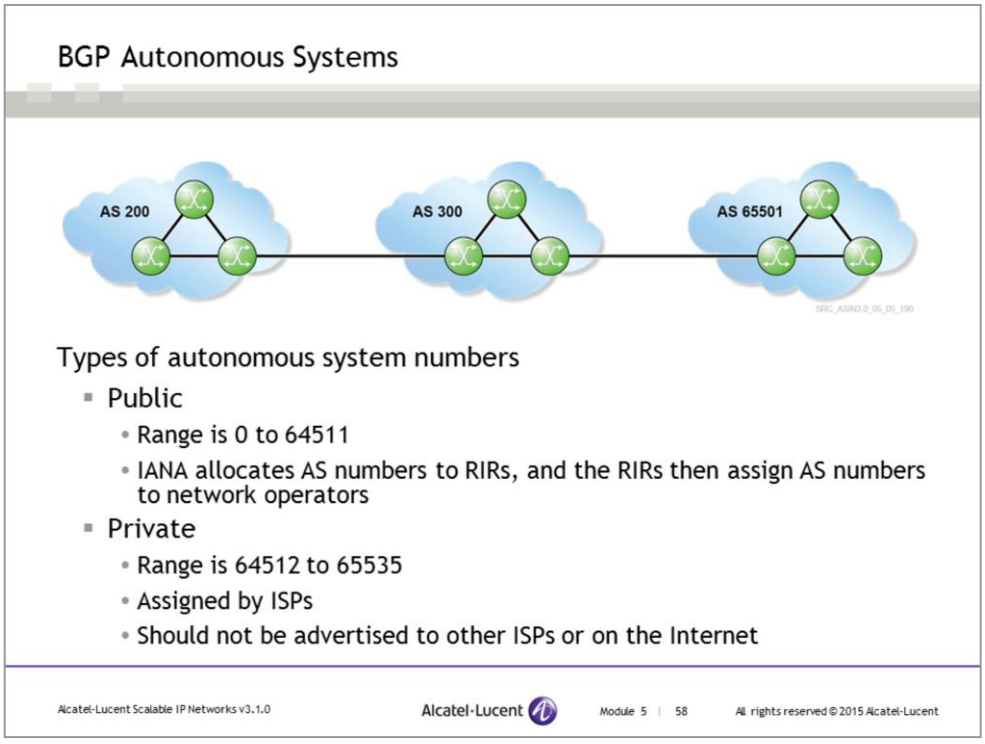
BGP is scalable to the following characteristics:

- Large number of autonomous systems
- Large number of neighbors
- Large volume of table entries
- High rate of change

BGP has proven scalability. BPG is the protocol of choice for service providers and runs on their Internet routers. The protocol is the fundamental building block of the Internet and is used by every service provider in the world for service-provider interoperability. BGP is the most feature-rich and scalable routing protocol in use today. It supports the current requirements of the Internet and, with extended capabilities such as multiple protocol families and extended AS numbers, is well-positioned for the future.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Public autonomous systems

- IANA allocates AS numbers to RIRs, and the RIRs then assign AS numbers to network operators
- Must be used to connect to other autonomous systems in the Internet
- Range is 0 to 64511

Private autonomous systems

- Are assigned by ISPs, local administrators, and so on
- Should not be advertised to other ISPs or on the Internet
- Range is 64512 to 65535

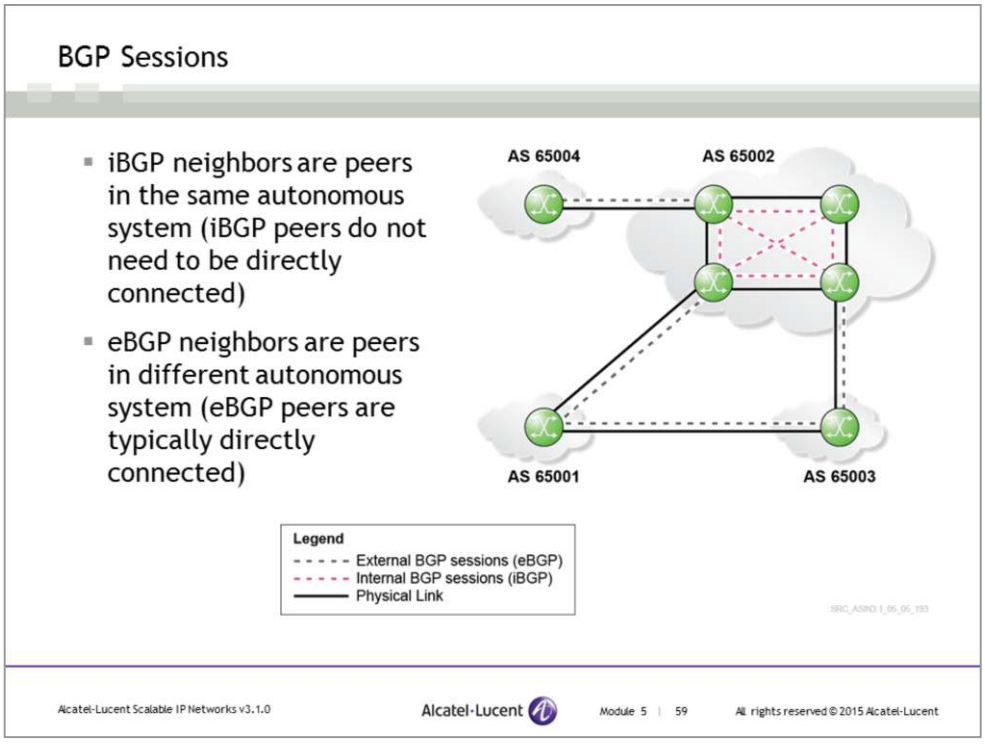
Regional Internet Registries

IANA is the umbrella organization. Regional Internet Registries (RIRs) are nonprofit corporations established for the purpose of administration and registration of IP address space and AS numbers on behalf of the IANA. There are five RIRs.

Registry	Geographic Region
AfriNIC	Africa, portions of the Indian Ocean
APNIC	Portions of Asia, portions of Oceania
ARIN	Canada, the United States, and many Caribbean and North Atlantic islands
LACNIC	Latin America, portions of the Caribbean
RIPE NCC	Europe, the Middle East, Central Asia

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



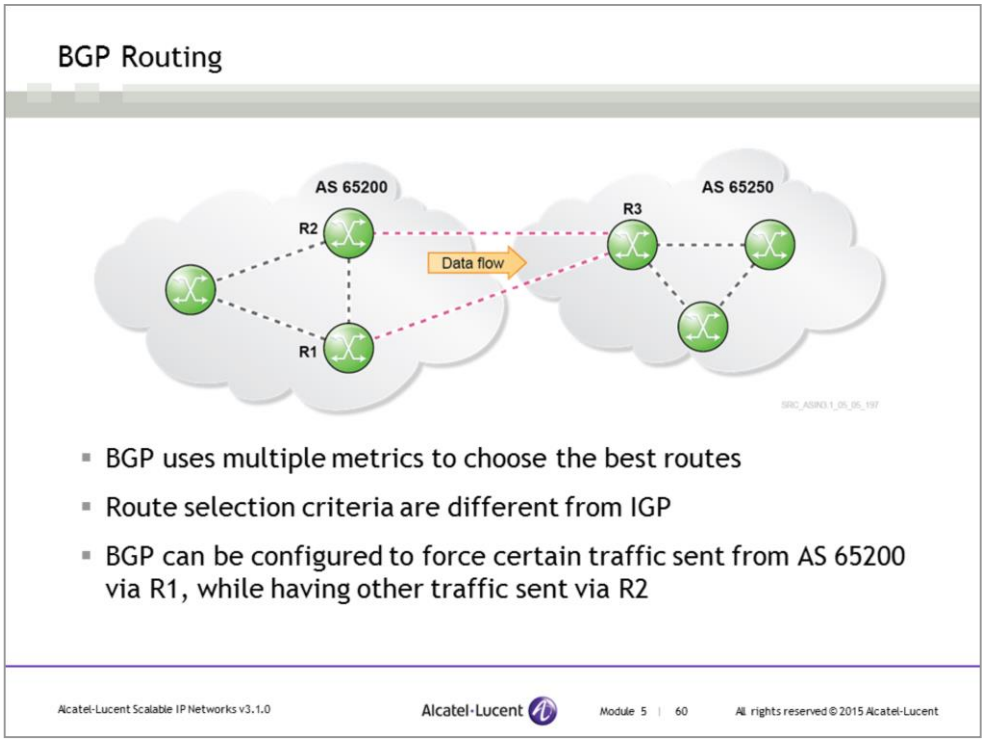
There are two types of BGP neighbor relationships: eBGP and iBGP. Regardless of the type, a BGP session between two devices is referred to as a neighbor or peer session. A BGP router is also referred to as a BGP speaker.

A session between two devices in different autonomous systems is referred to as an external BGP or eBGP session. Typically, devices with an eBGP session are directly-connected but it is not mandatory. Because the devices are in different autonomous systems, the administration of each device is usually handled separately. Therefore, you should ensure that the configuration parameters match so that peering will succeed.

A session between two devices in the same autonomous system is referred to as an internal BGP or iBGP session. Typically devices with an iBGP session are not directly-connected because they may be located across the country or on the other side of the globe. However, the device must know how to reach its iBGP peer from the routing table. Because the devices are in the same autonomous system, the administration of each device is usually handled by the same organization. You need to ensure that the configuration parameters match so that peering will succeed.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



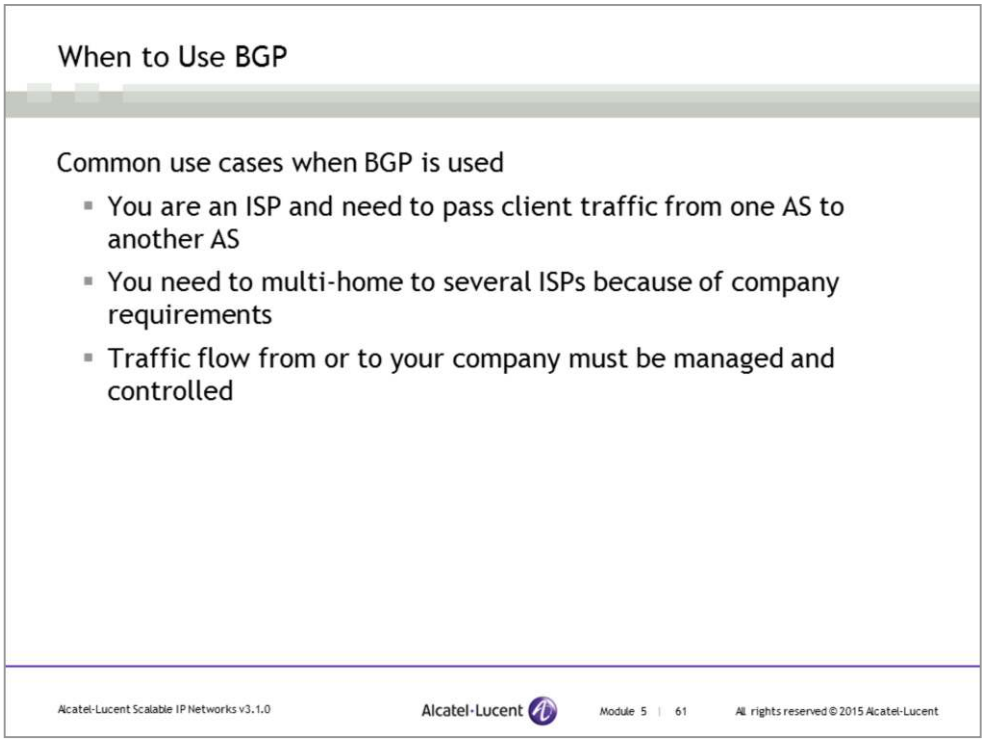
The criteria that BGP uses for route selection is very different from IGP. In an IGP environment, the routes are selected based on one metric, such as cost or hop count. However, when you use BGP to route traffic between organizations, the choice may not be solely made based on the shortest path, but must consider financial, security, and geographical factors.

In this slide, R3 has two equal-cost paths from AS 65250 to AS 65200, one through its eBGP session to R2 and another one through its eBGP session to R1. Because both R1 and R2 are in the same AS, the path cost for each eBGP session is the same.

However, BGP can be configured to prefer certain routes advertised over one link, while having other routes advertised over another link. This is done by changing the BGP attributes. BGP attributes can be used to influence BGP routing policies. Note that the use of additional attributes can complicate the configuration of BGP. More details on BGP are discussed Alcatel-Lucent's BGP course.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

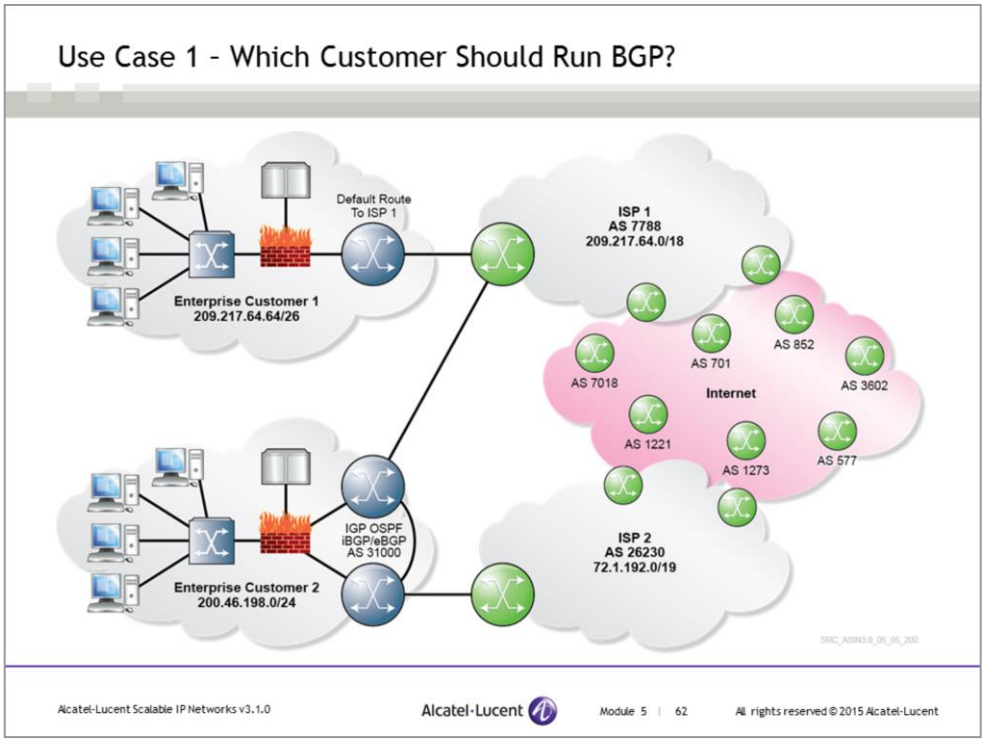


BGP can accommodate virtually any number of policies. This flexibility can be something of a double-edged sword. BGP is administratively more complex than IGP. BGP updates include path information that is used for routing policy enforcement and loop detection between ASs.

Adding to the complexity of BGP is the fact that topology and routing table sizes become much larger than in an IGP environment. The increased size of the tables means that factors such as CPU loading, memory utilization, update generation, and route processing have greater implications in BGP. Therefore, BGP routes should NEVER be redistributed into any other routing protocols.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



ISP 1 and ISP 2 will be running BGP since they are acting as transit providers for their customers to the Internet. The Internet is made up of thousands of routers and AS numbers. Larger Internet providers interconnect and share routes with each other using eBGP. There are two enterprise customers shown in the diagram.

Customer 1 has a single connection to ISP 1 and is borrowing address space from that provider (subnet 209.217.64.64/26). This customer will use a default-route to ISP 1. ISP 1 will have a route back to its customer's subnet using either static-routes or a dynamic routing protocol. ISP 1, using BGP, will advertise its aggregate network of 209.217.64.0/18 to its upstream providers in the Internet cloud using eBGP. From the Internet, it will appear as though 209.217.64.64/26 is not being advertised, and only the aggregate will be seen (209.217.64.0/18) coming from AS 7788, which belongs to ISP 1 (in most cases, best practice is to summarize and not leak specific subnets).

Customer 2 has a two connections for redundancy: one to ISP 1 and one to ISP 2. Customer 2 has its own IP address block they received from the American Registry for Internet Numbers (ARIN). In the previous slide it was mentioned that, in most cases, there is no need to run a complex routing-protocol like BGP unless you have multiple connections to the Internet like Customer 2. Customer 2 requires redundant connectivity to the Internet because it either needs the extra bandwidth or simply cannot afford to be offline from the Internet if a link fails. The server in the Customer 2 cloud could be offering important files and must be online for continuous operation.

Customer 2 advertises its network 200.46.198.0/24 via BGP. From the Internet, it appears as though the network is coming from AS 31000, which was assigned to Customer 2 from ARIN. In fact, other BGP routers on the Internet will see 200.46.198.0/24 with two 'paths'. One path will be 200.46.198.0/24 from AS 31000, 26230 (through ISP 2) and another path for this same address space from AS 31000, 7788 (through ISP 1).

Since BGP is a path-vector protocol, in most cases, the route selection used by the Internet will make its route selection to Customer 2 based on the shortest AS-PATH. There are several route-metrics used in BGP for route selection and they are covered in detail in Alcatel-Lucent's BGP

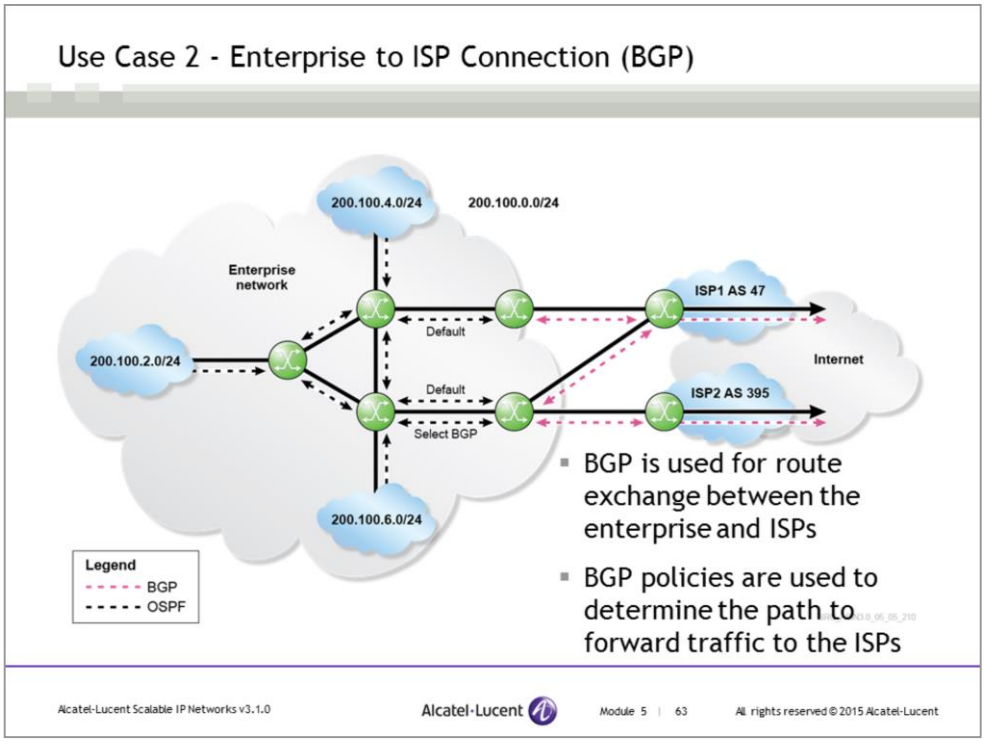
 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

course.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



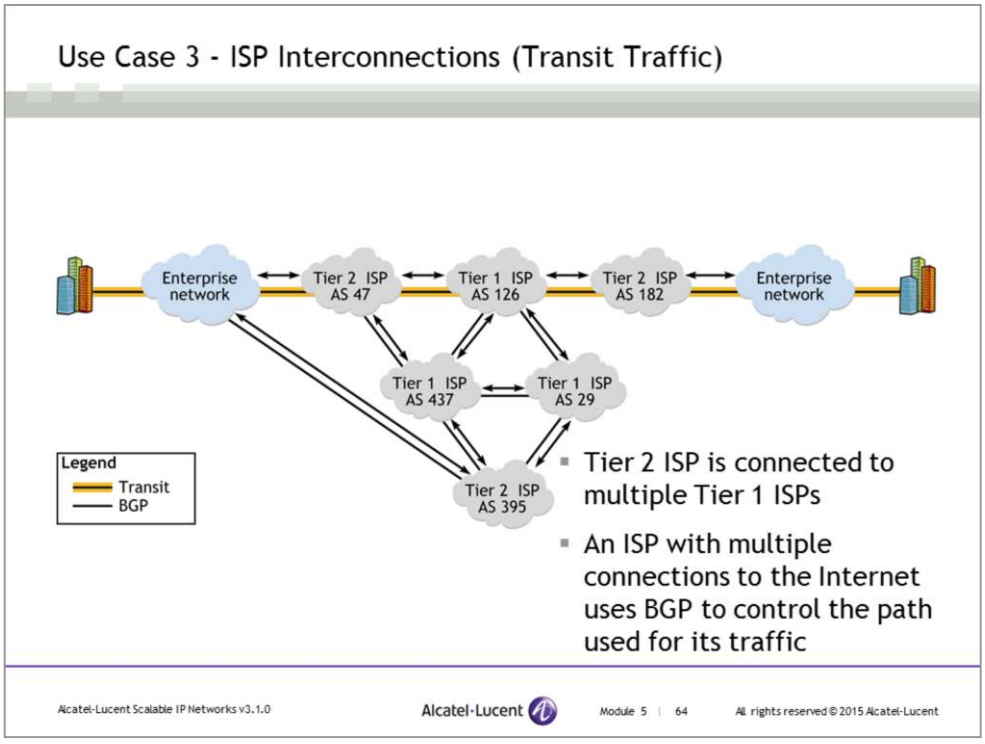
In this slide, the enterprise has a large OSPF network with multiple Local Area Network (LAN) segments. The enterprise also has multiple connections to two ISPs (AS 47 and AS 395). In this configuration, the enterprise will often run BGP to manage the connections with their ISPs. BGP policies are used to determine the path that is used for traffic to leave the enterprise. One ISP may be preferred for some routes, or one ISP may be used as a primary connection to the Internet with the other ISP used as a backup.

Within the enterprise network, internal routing information is exchanged with OSPF. The enterprise networks are summarized as 200.100.0.0/20, and advertised to the ISPs and onwards to the Internet with BGP. In this scenario, the enterprise uses a private AS number and its routes are advertised by the ISPs using their AS numbers.

The full set of Internet routes is not exported into OSPF. Instead, a default route is advertised by the Internet-connected routers. Some subsections of the BGP routes that are received may be advertised into the enterprise in order to influence the route for that traffic to egress the enterprise network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



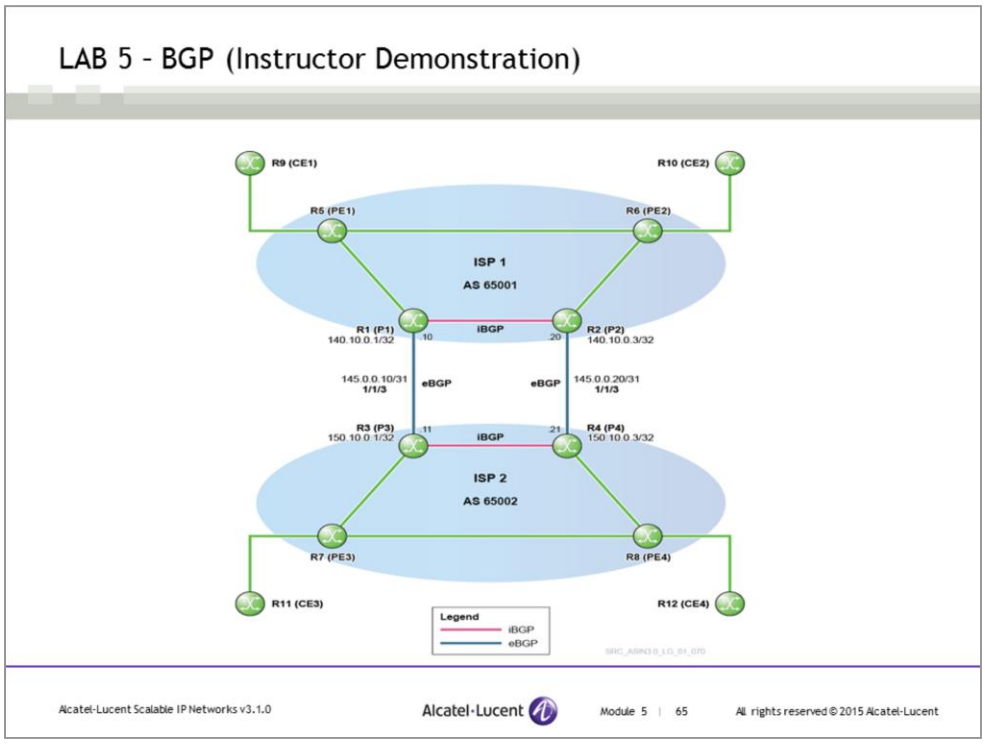
In this slide, an enterprise is connected to its two ISPs (AS 47 and AS 395). Routing information is exchanged between the enterprise and the two ISPs using BGP. Both ISPs are Tier 2 ISPs, which means that they purchase transit capacity from one or more Tier 1 ISPs. Similar to the enterprise, the Tier 2 ISPs pay the Tier 1 providers to carry their traffic.

The Tier 1 providers carry transit traffic. This is traffic that originated outside of their network and has a destination outside of their network. A Tier 2 ISP may be connected to more than one Tier 1 ISP, or may have transit arrangements with other Tier 2 ISPs. Multiple connections are often used to provide the ISP with a redundant path to all Internet destinations.

An ISP with multiple connections to the Internet usually needs to control the path used for its traffic. The reason may be to ensure the shortest path, but often is related to cost or other considerations.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Section Objectives

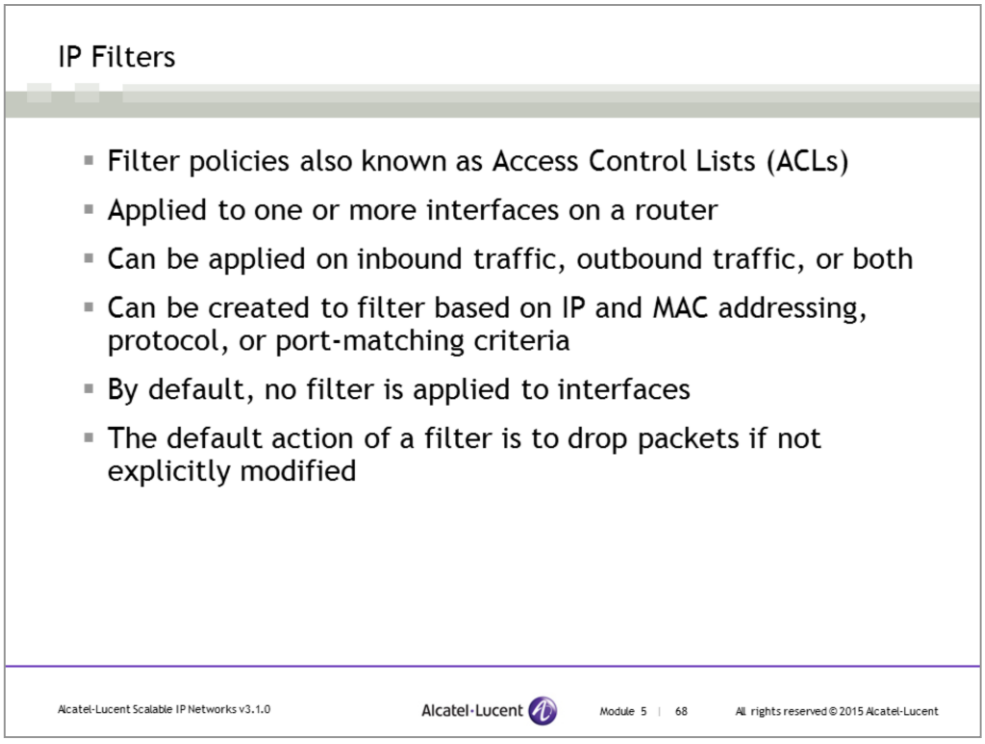
After successful completion of this section, you will be able to:

- Describe the use of IP filters
- Configure an IP filter and apply it to a router interface
- Use the **show** command to verify the IP filter configuration

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent



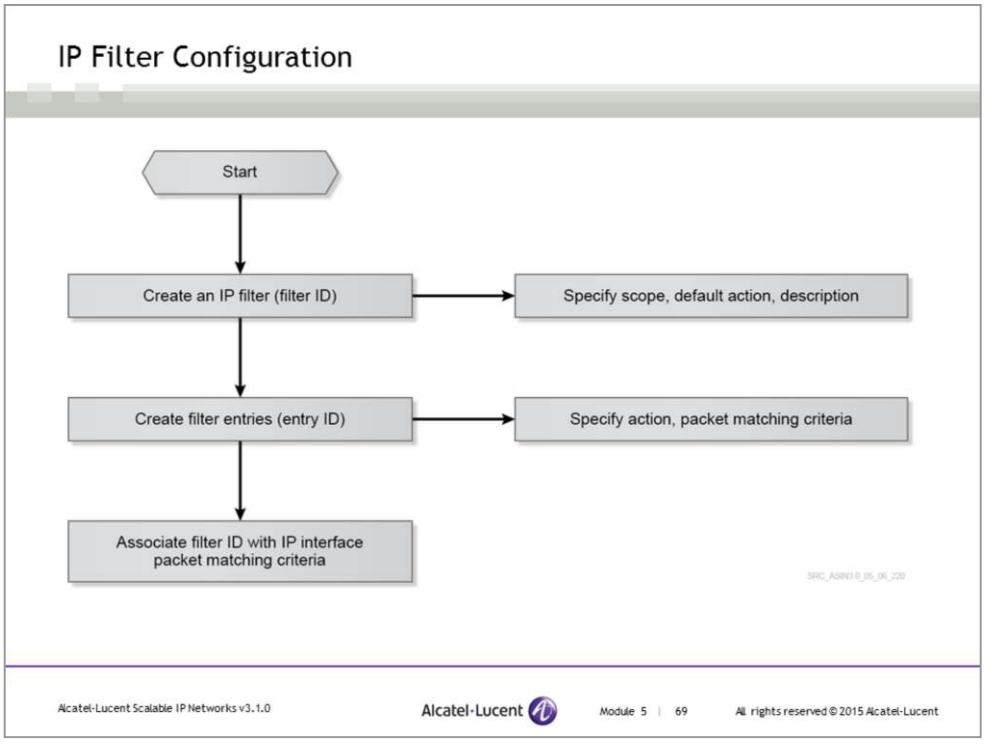
Filters, also known as access control lists (ACLs), are templates that are applied to services or network ports to control network traffic into (ingress) or out of (egress) a SAP or network port based on IP and MAC match criteria. Filters are applied to examine packets that are entering or leaving a SAP or network interface. Filters can be used on several interfaces. The same filter can be applied to ingress traffic, egress traffic, or both. Ingress filters affect only inbound traffic that is sent to the routing complex, and egress filters affect only outbound traffic that is sent from the routing complex.

Configuring a service or network port with a filter is optional. If a service or network port is not configured with filter policies, all traffic is allowed on the ingress and egress interfaces. By default, no filters are associated with services or interfaces; the filters must be explicitly created and associated with the service or interface. When you create a filter, default values are provided although you must specify a unique filter ID for each new filter policy, each new filter entry, and the associated actions. The filter entries specify the filter match criteria. Only one ingress filter policy and one egress filter policy can be applied to a network interface at a time.

Network filter policies control the forwarding and dropping of packets based on IP match criteria. Note that IP match criteria are applied to IP packets only. The default action in the filter policy applies to non-IP packets. If the default action is not explicitly configured, then the default action is to drop all non-matching packets. As an alternative action, the filter might simply allow the packet to be forwarded normally, or it might forward it to a different next hop than would be indicated by the router's normal forwarding table.

 All rights reserved © 2015 Alcatel-Lucent

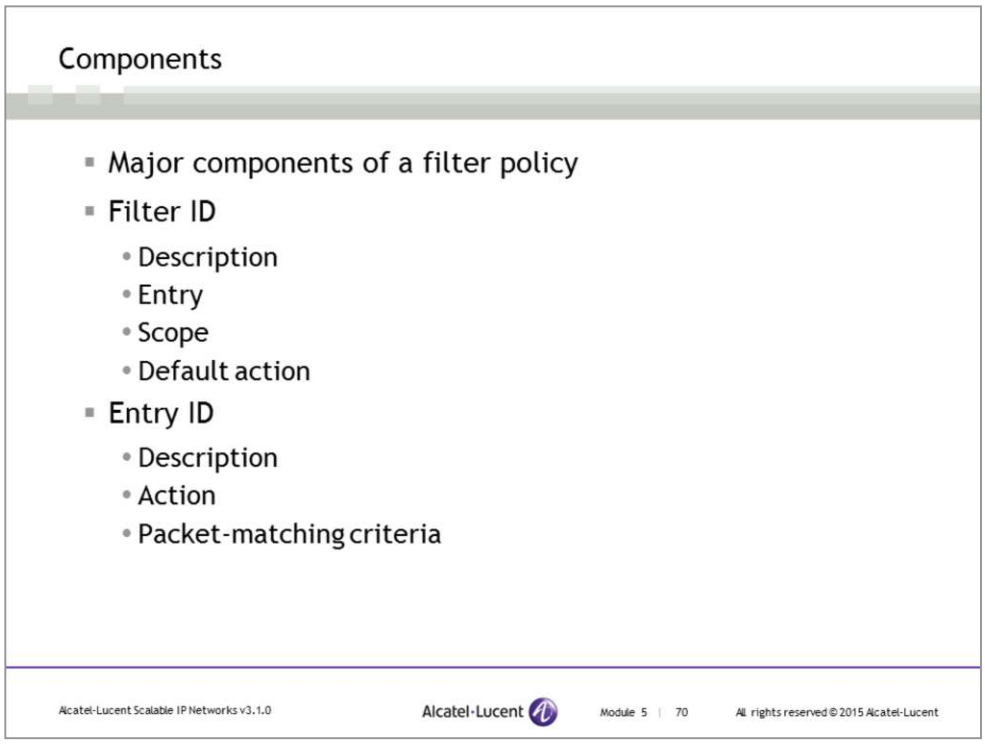
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This slide shows the process used to create a filter policy. The filter must be created with its associated scope, description, and default action. Then, individual filter entries need to be created to specify what criteria the filter will examine in the IP packets. Finally, the policy must be applied to an interface.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Filter ID

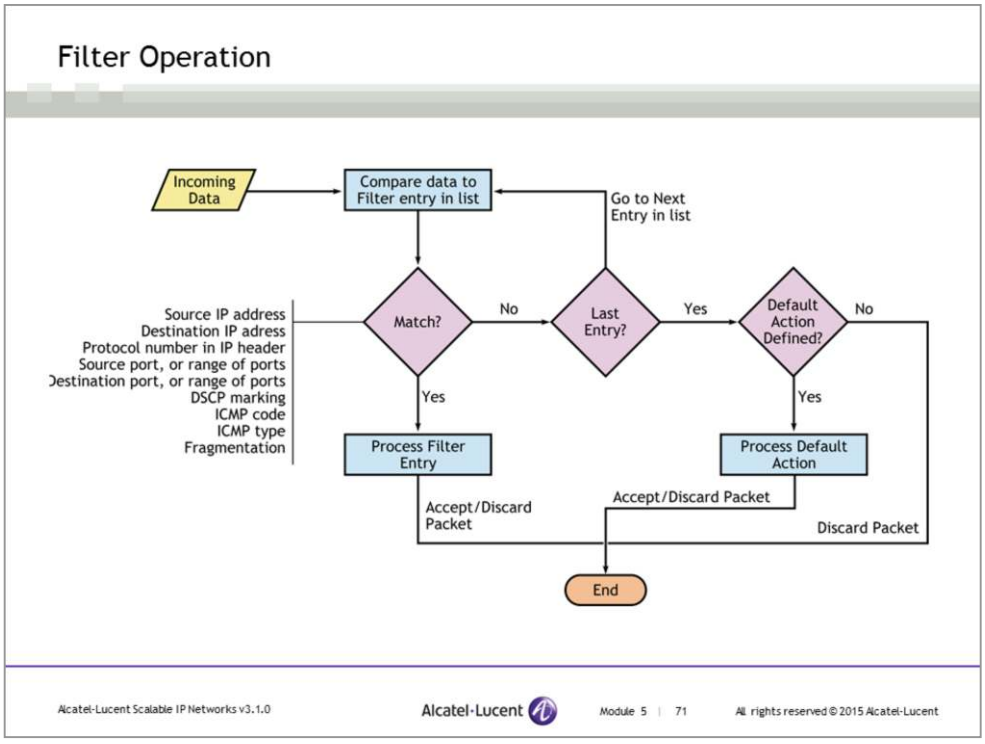
- Filter ID (mandatory) — The value that identifies the filter
- Description (optional) — A brief overview of the filter features
- Scope (mandatory) — A filter policy must be defined with an exclusive scope for one-time use, or a template scope, which enables the policy to be used with multiple interfaces.
- Default action (mandatory) — The action to be applied to packets when no action is specified in the IP or MAC filter entries, or when the packets do not match the specified criteria.

Entry ID (one or more) represents a collection of filter match criteria. Packet matching starts the comparison process with the criteria specified in the lowest entry ID. Entries identify attributes that define matching conditions and actions. Packets must match all of the criteria in the entry for the specified action to be performed. Each entry consists of the following components:

- Entry ID (mandatory) — The value determines the order of the entry IDs in a specific filter ID. Packets are compared to entries in an ascending order, starting with the lowest entry ID.
  - Description (optional) — A brief overview of the entry ID criteria.
  - Action (mandatory) — An action parameter must be specified for the entry to be active. A filter entry without a specified action parameter is inactive.
  - Packet-matching criteria — You can enter and choose criteria to create a specific template through which packets are compared, and forwarded or dropped, depending on the specified action.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A filter policy compares the match criteria specified in a filter entry to the packets that are entering the system, in the order that the entries are numbered in the policy. When a packet matches all of the parameters in a particular filter entry, the system performs the specified action to drop or forward the packet. If a packet does not match the entry parameters, the packet continues through the filter process. If the packet does not match any of the entries, the system performs the specified default action (i.e. drops the packet unless a different default action is configured). A single filter can have many entries, each with its own criteria to match. A packet will be examined against each entry, so the more entries that exist, the more processing required.

Each filter policy is assigned a unique filter ID and is defined with:

- Scope (indicates whether this policy can be used only once or can be used many times)
- Default action (such as Accept or Discard)
- Description (explains what the filter is for)
- Filter name that can be optionally used in CLI to reference this filter policy instead of filter ID
- At least one filter entry (the actual matching criteria)

Each filter entry contains:

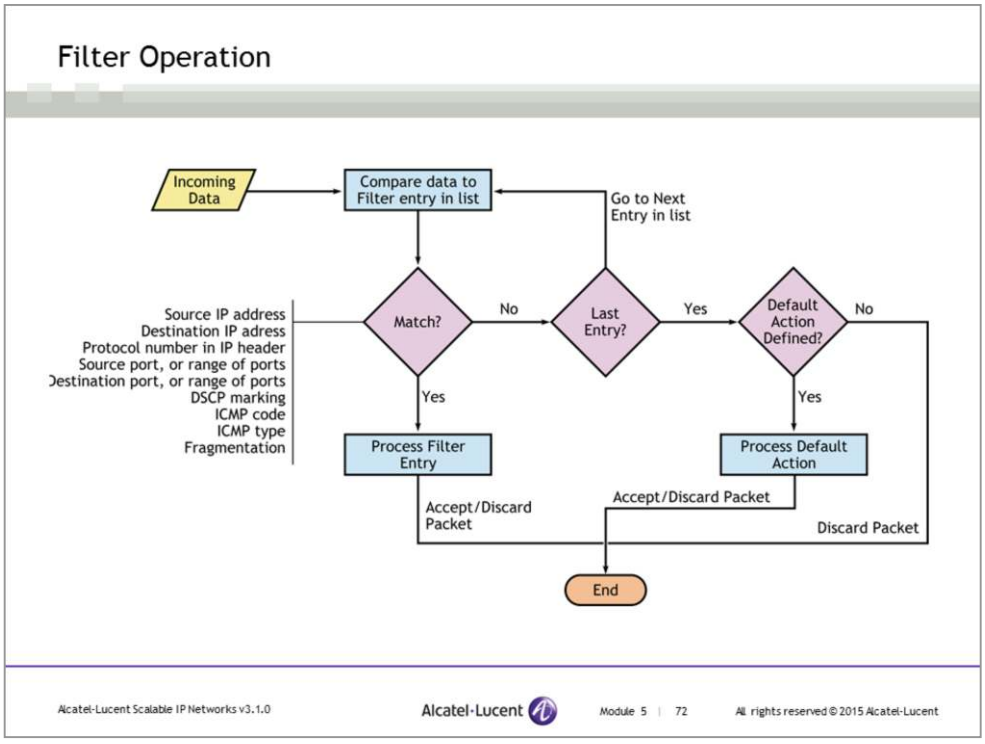
- At least one match criterion (IP address source or destination, upper-layer protocol, upper-layer protocol port, etc)
- An action (such as Accept or Discard)

As few or as many match parameters can be specified as required, but all of the conditions in the entry must be met for the packet to be considered a match and the specified entry action performed. The process stops when the first complete match is found. Then, the action defined in the entry is performed, that is, the packets that match the criteria are dropped or forwarded.

(…continued on next slide)

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



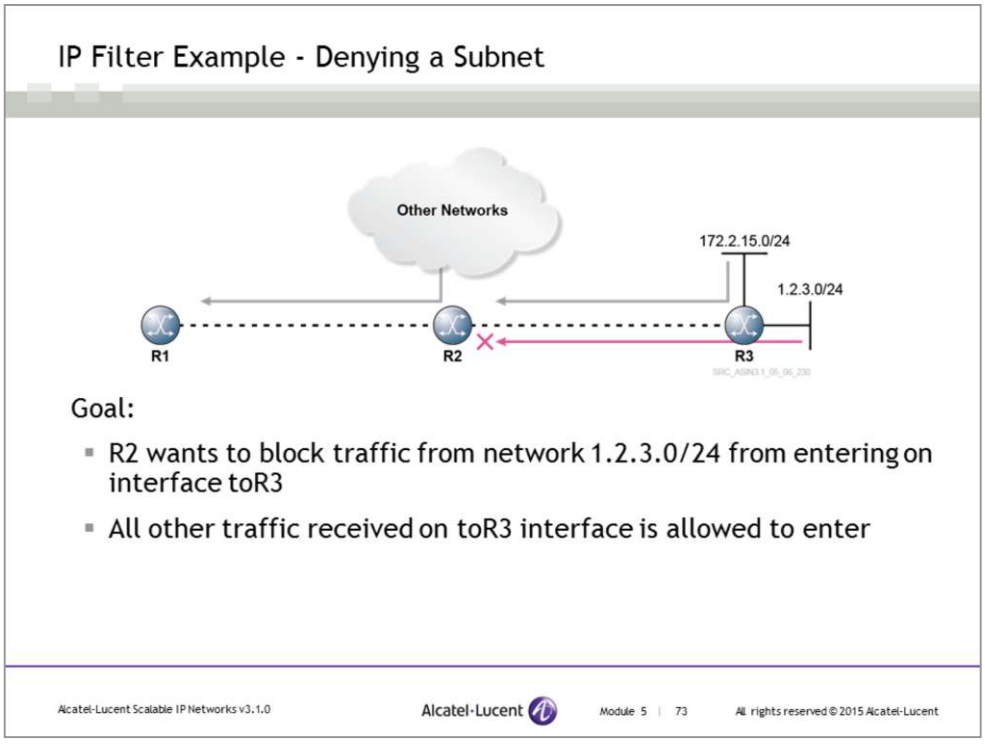
(…continued from previous slide)

Match criteria to drop or forward IP traffic include:

- Source IP address and mask — The values can be entered as search criteria. Address ranges are configured by specifying network prefix values. The prefix mask length is expressed as an integer (range 0 to 32).
- Destination IP address and mask — The values can be entered as search criteria. Address ranges are configured by specifying network prefix values. The prefix length is expressed as an integer (range 0 to 32).
- Protocol — The protocol (for example, TCP, UDP) allows the filter to search for the specified protocol.
- Source port/range — The source port number or range allows the filter to search for the matching TCP or UDP port and range values.
- Destination port/range —The destination port number or range allows the filter to search for the matching TCP or UDP values.
- DSCP marking — A DSCP marking allows the filter to search for the specified DSCP.
- ICMP code — An ICMP code allows the filter to search for the matching ICMP code in the ICMP header.
- ICMP type — An ICMP type allows the filter to search for the matching ICMP type in the ICMP header.
- Etc.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

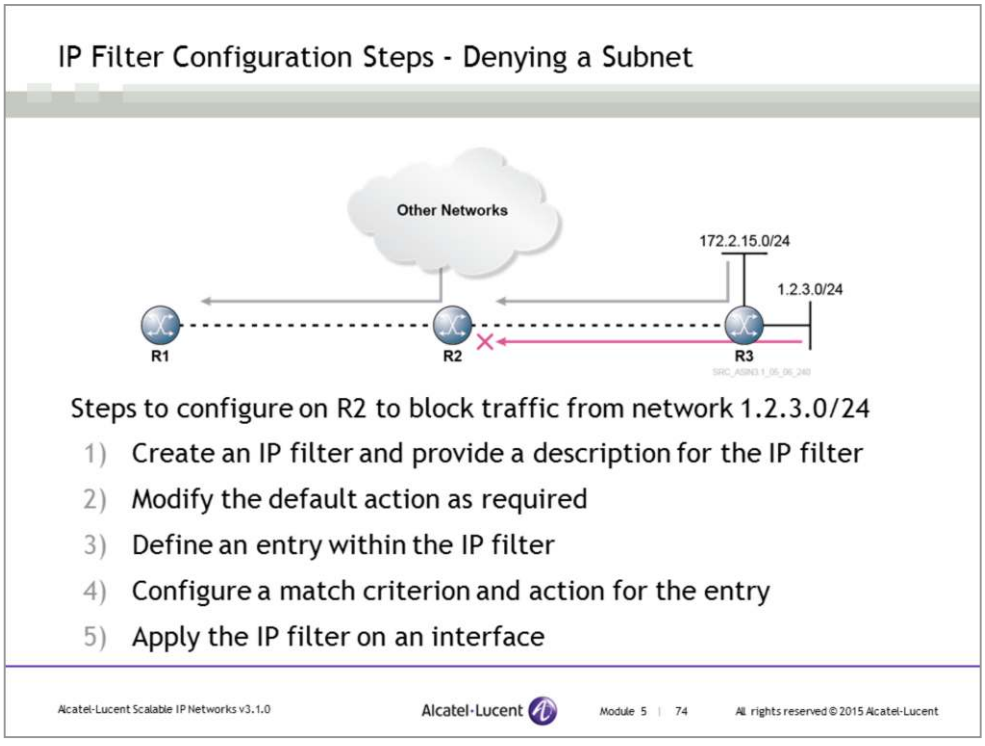


In this slide, R2 is configured to stop traffic from network 1.2.3.0/24 from entering the router on interface toR3. This filter blocks all traffic received from that network from passing through to any other network in the topology.

All other traffic received on the toR3 interface is allowed to enter, which is the default action.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

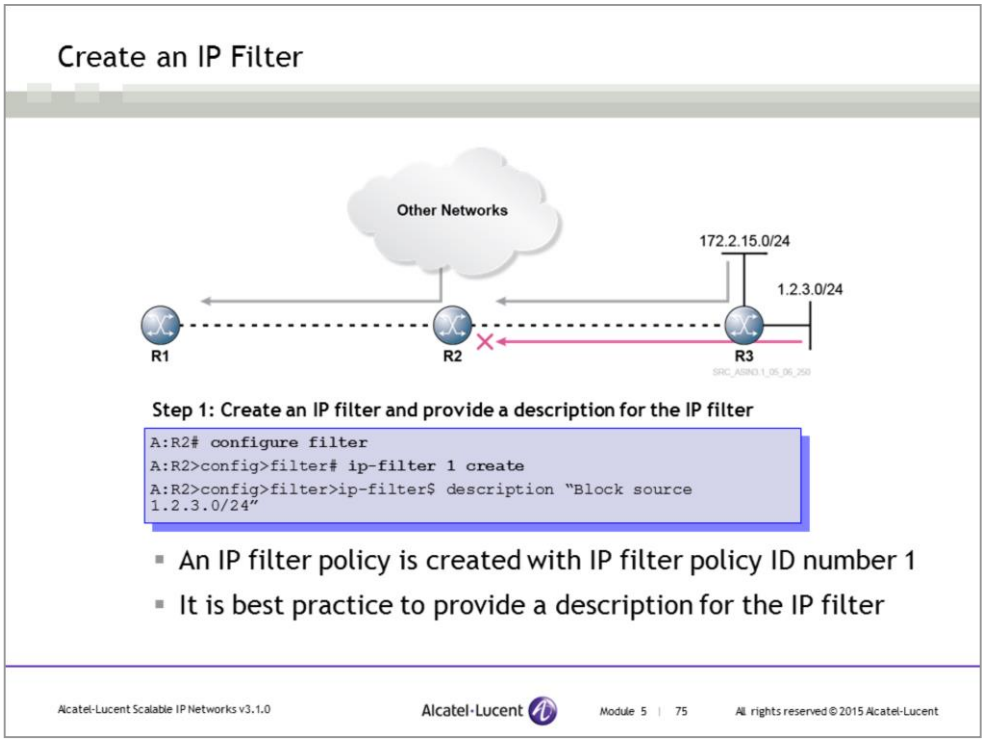


In this case, an IP filter can be used to block traffic from a specific network.

Within a filter policy, you must configure filter entries that contain criteria against which ingress and/or egress traffic is matched. The action specified in the entry determines how packets are handled, either dropped or forwarded.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

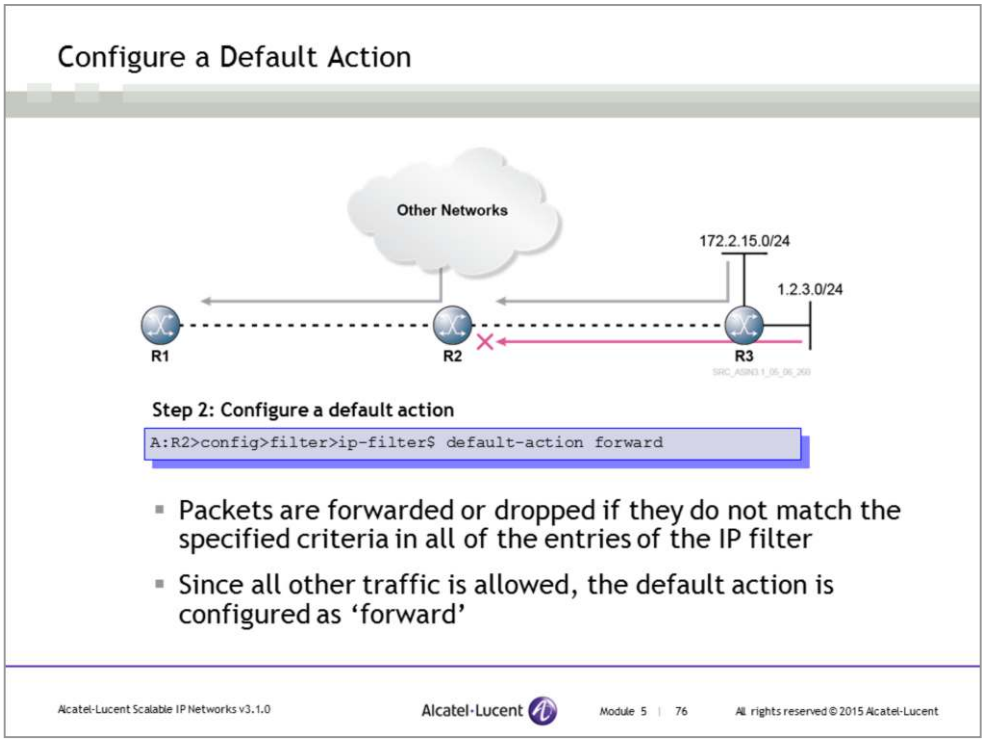


This command creates a configuration context for an IP filter policy. An IP filter policy specifies a forward or drop action for packets, based on the specified match criteria. An IP filter policy (also called an Access Control List (ACL)) can be applied to multiple services or multiple network ports when the scope of the policy is a template. Changes to the existing policy, using the subcommands, are applied immediately to all services to which this policy applies. Therefore, when many changes to an IP filter policy are required, it is best practice to copy the policy to a work area. You can modify the work-in-progress policy and then replace the original filter policy with the revised policy. Use the **config filter copy** command to maintain policies.

The 'no' form of the command is used to delete the IP filter policy. A filter policy cannot be deleted until the policy is removed from all network ports to which the policy was applied.

All rights reserved © 2015 Alcatel-Lucent

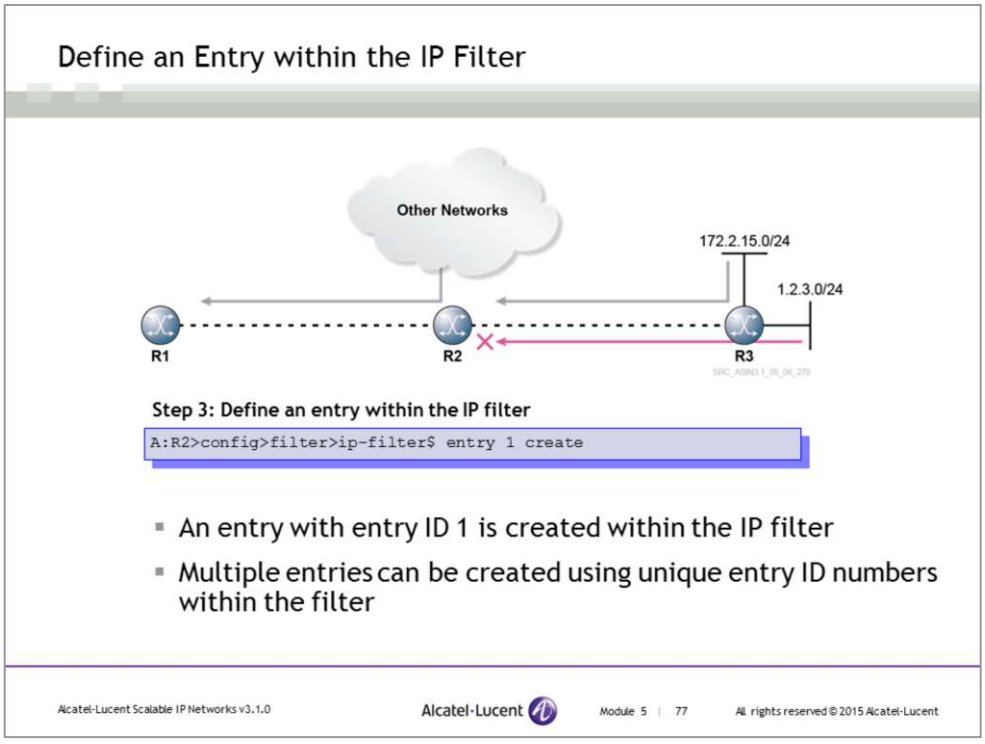
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This command specifies the action to be performed when the packets do not match the specified criteria in all of the entries of the IP filter. When multiple default-action commands are entered, the last command overwrites the previous command.

All rights reserved © 2015 Alcatel-Lucent

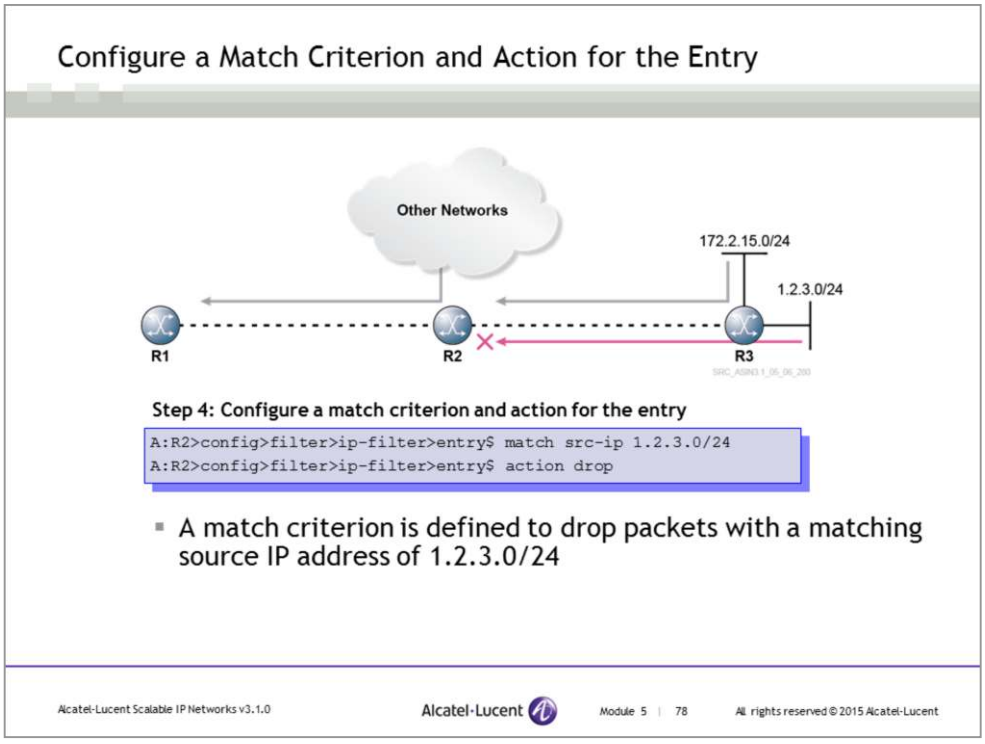
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This command allows you to create or modify an IP filter entry. Multiple entries can be created using unique entry ID numbers in the filter. The Alcatel-Lucent 7750 SR exits the filter at the first match and performs the action according to the accompanying action command. For this reason, entries must be sequenced correctly from most explicit to least explicit. An entry may not have any match criteria (in which case, everything matches) but must have at least the action keyword for the entry to be considered complete. Entries without the action keyword are rendered inactive. The 'no' form of the command removes the specified entry from the IP filter.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



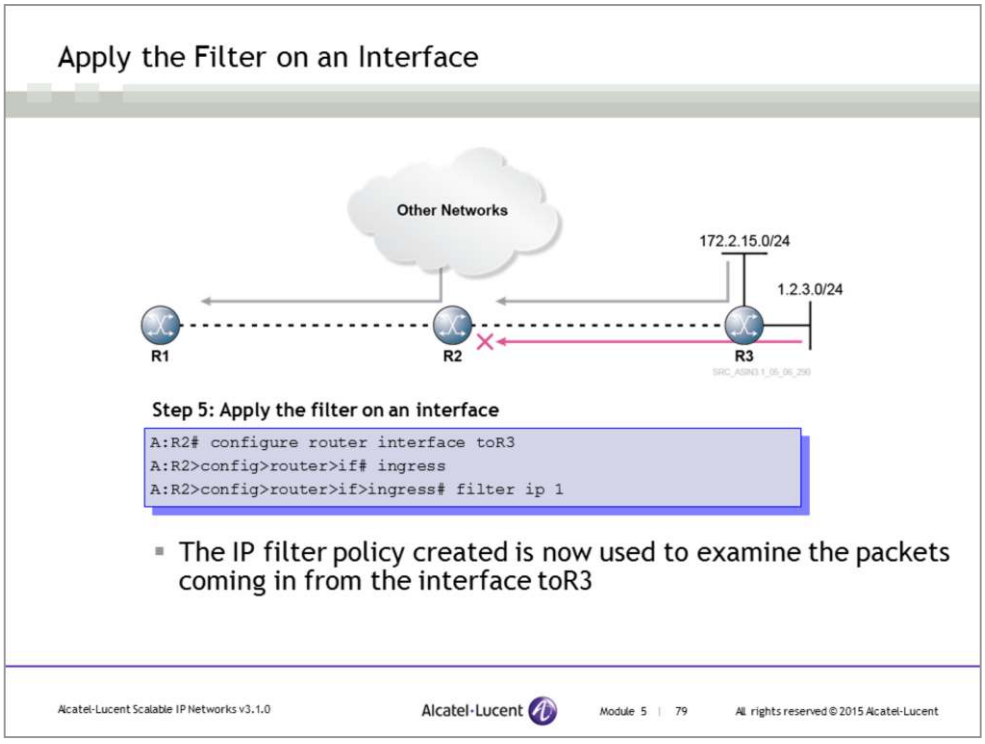
This command provides the context to enter match criteria for the filter entry. When the match criteria are met, the action associated with the match criteria is performed.

If more than one match criterion within a match statement is configured, then all criteria must be met (AND function) before the action that is associated with the match is performed.

A match context may consist of multiple match criteria, but multiple match statements cannot be entered for an entry. The no form of the command removes the match criteria for the entry ID.

All rights reserved © 2015 Alcatel-Lucent

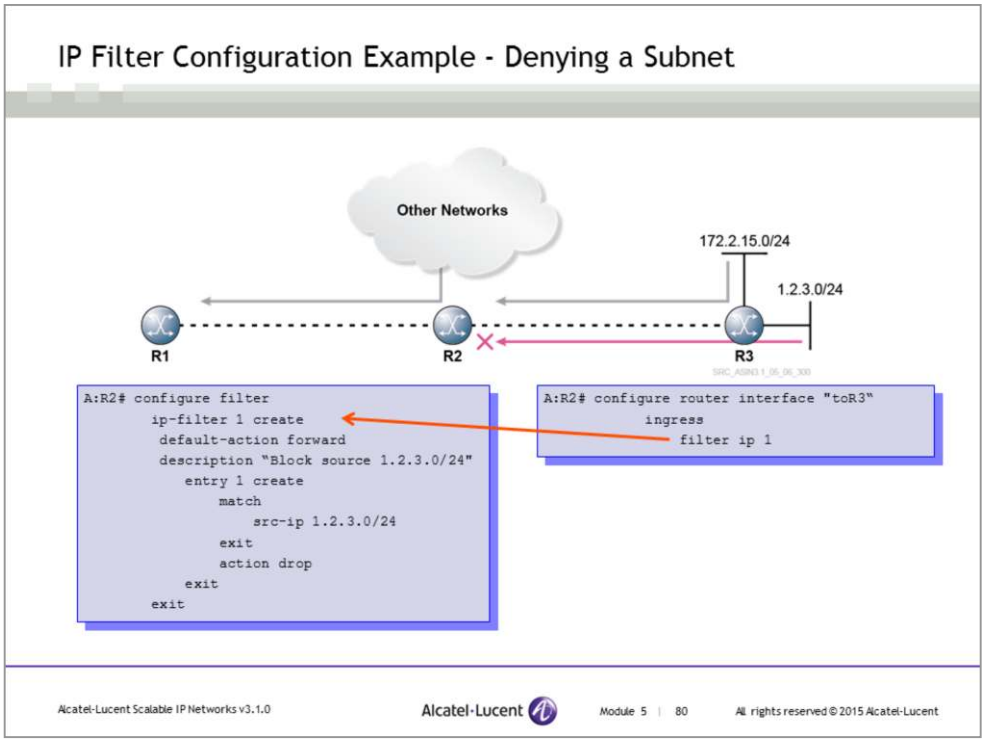
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



This command associates an IP filter policy with an IP interface. Filter policies control packet forwarding and dropping based on IP match criteria. The IP filter policy with the specific filter ID must be pre-configured before this command can be executed. If the filter policy with the specific filter ID does not exist, an error occurs. Only one filter ID can be specified.

 All rights reserved © 2015 Alcatel-Lucent

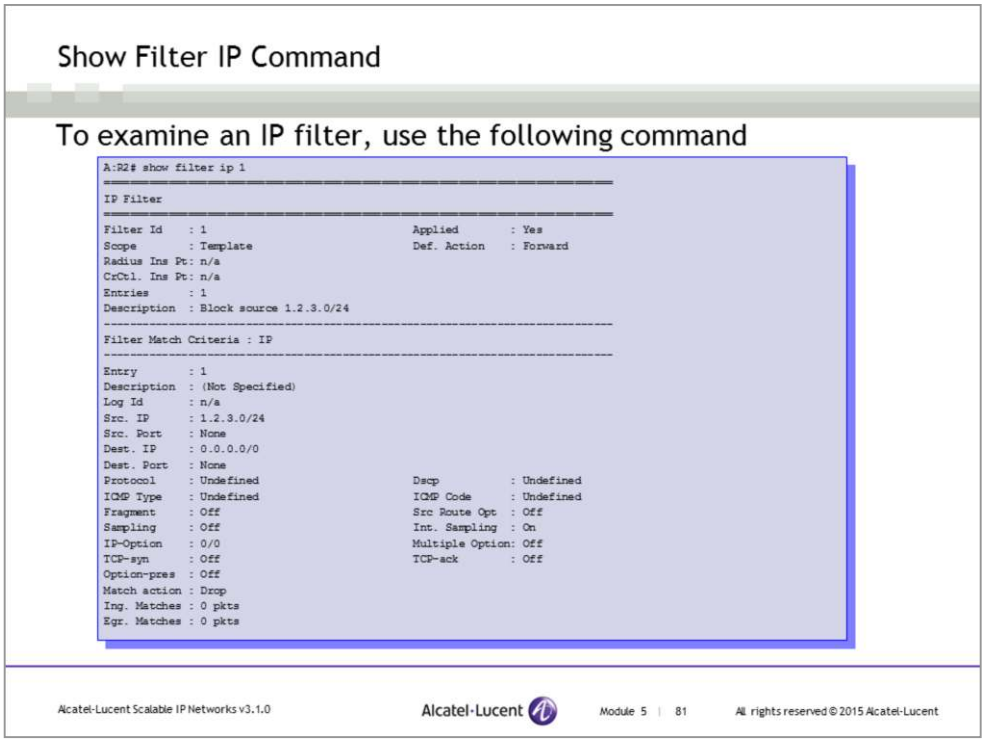
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



R2 is configured to stop traffic from network 1.2.3.0/24 from entering the router on interface toR3. This filter blocks all traffic received from that network from passing through. All other traffic received on the toR3 interface is allowed to enter, which is the default action.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

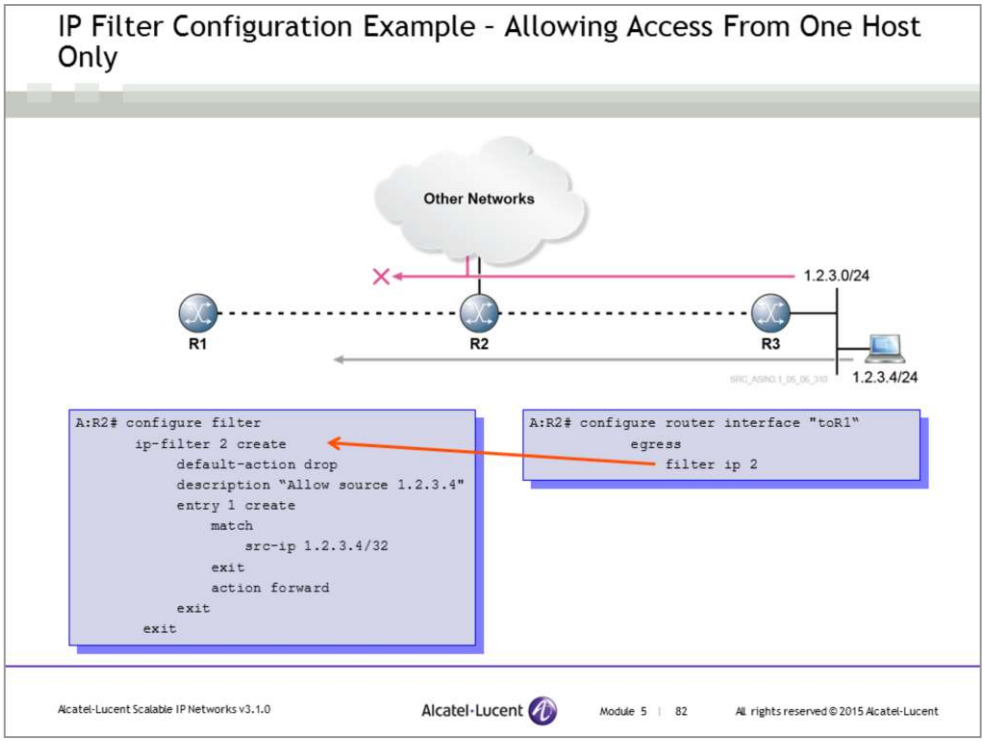


In this slide, IP filter 1 was created. In the filter, the default action is to forward IP packets that do not meet the explicit match settings.

In the match settings, the filter checks for all traffic sourced from IP subnet 1.2.3.0/24. If this criterion is met, the packet is dropped.

All rights reserved © 2015 Alcatel-Lucent

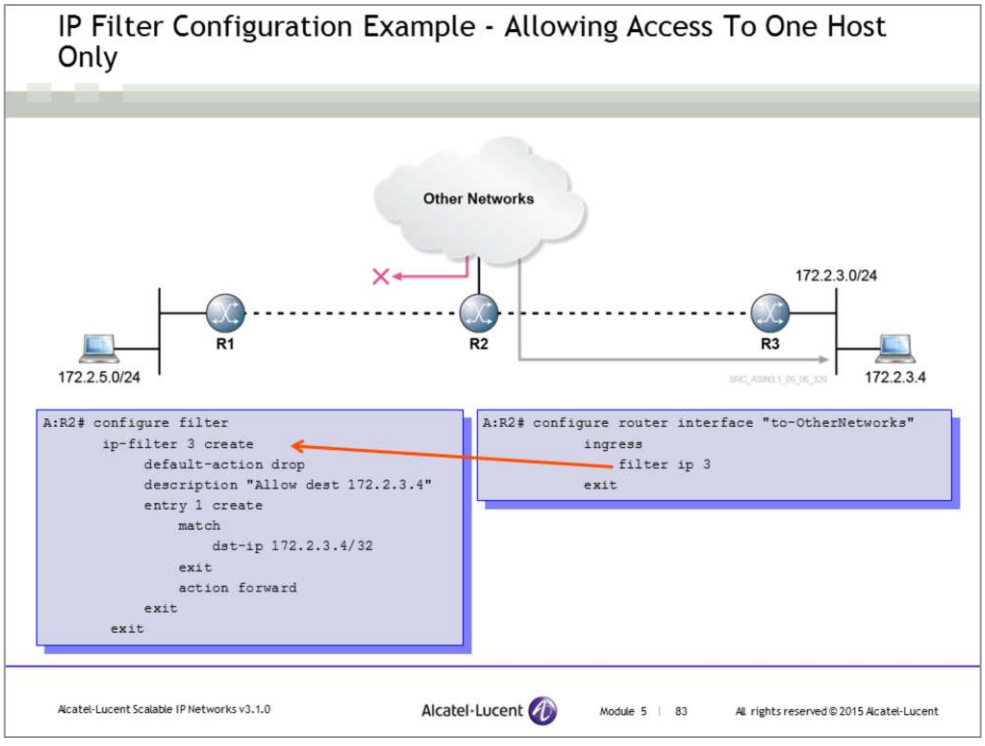
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In this slide, a new filter has been created to allow only traffic from host 1.2.3.4 to reach R1 by applying the filter on the egress direction of R2's interface to R1. All other traffic received from R3 to R1 will be dropped. However, traffic from R3 to Other Networks will be accepted.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

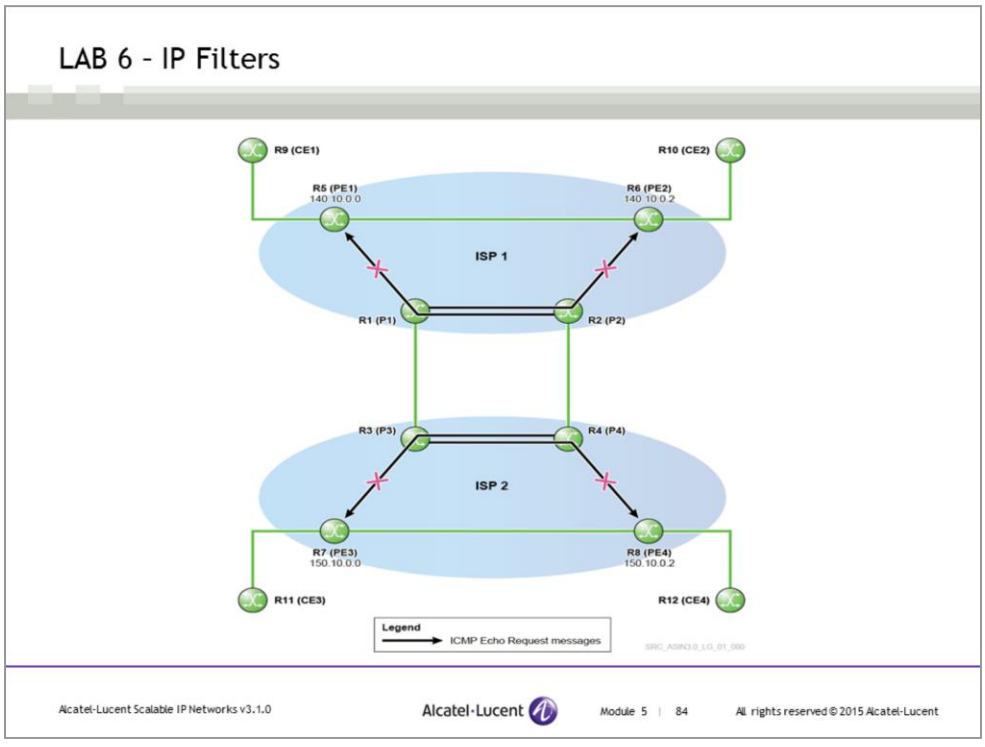


In this slide, traffic from Other Networks can only be sent to server 172.2.3.4. Traffic from Other Networks to any other address is dropped.

However, traffic from subnet 172.2.5.0/24 behind R1 can reach any client/server on subnet 172.2.3.0/24 behind R3.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

Module Summary

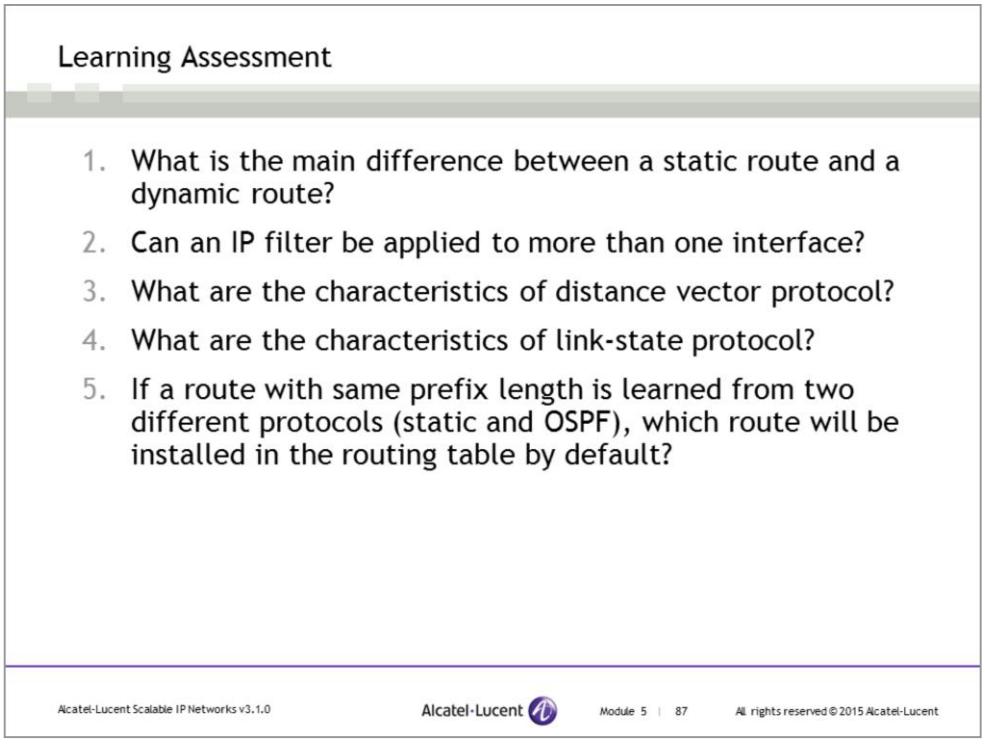
After successful completion of this module, you should be able to:

- Explain the concepts and purpose of IP routing
- Explain the purpose and configuration of static routes
- Describe the basic concepts of a dynamic routing protocol
- Describe the purpose and basic operation of OSPF
- Describe the purpose and basic operation of BGP
- Describe IP filter operation, components, configuration, and application

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 5 | 86
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

1. What is the main difference between a static route and a dynamic route?

A static route is manually configured, while a dynamic route is learned through a dynamic routing protocol.

2. Can an IP filter be applied to more than one interface?

Yes

3. What are the characteristics of distance vector protocol?

- Views the network topology from the neighbor's perspective
- The path with the lowest hop count (shortest distance) is the best path
- Frequent periodic updates (slow convergence)
- Passes copies of routing table to neighboring routers

4. What are the characteristics of link-state protocol

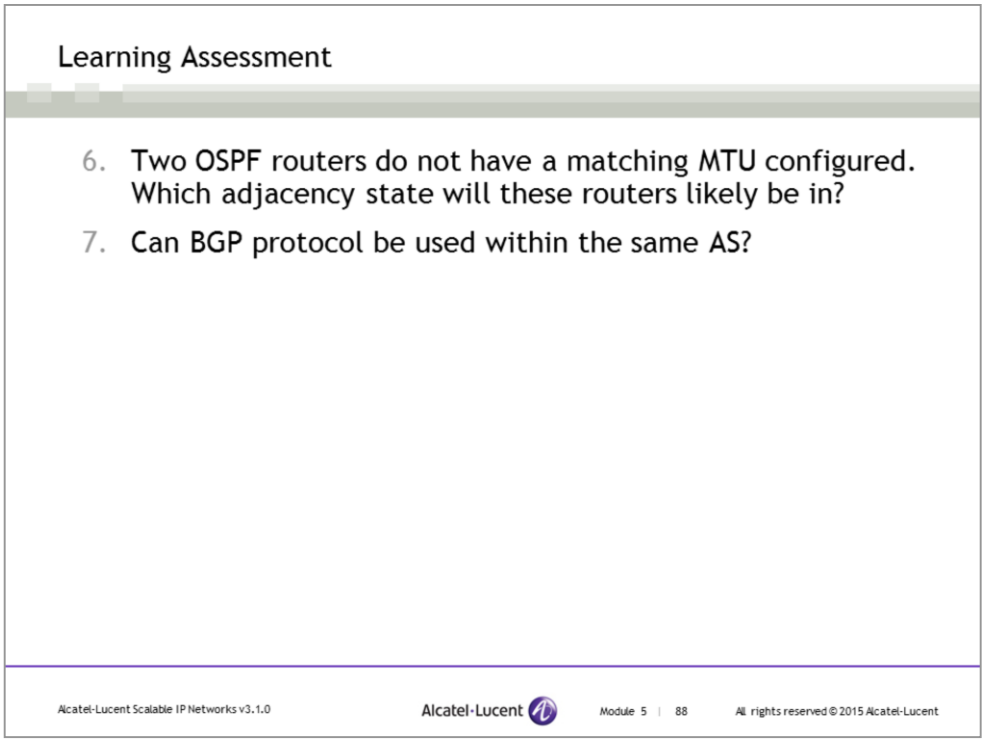
- Gets a common view of the entire network topology
- The path with the lowest cost is the best path
- Event-triggered updates (faster convergence)
- Passes link-state routing updates to other routers

5. If a route with same prefix length is learned from two different protocols (static and OSPF), which route will be installed in the routing table by default?

Static because it has a lower preference value than OSPF.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

6. The two OSPF routers do not have a matching MTU configured. What adjacency state will these routers likely be in?

Exchange Start state

7. Can BGP protocol be used within the same AS?

Yes, iBGP.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

 All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Objectives

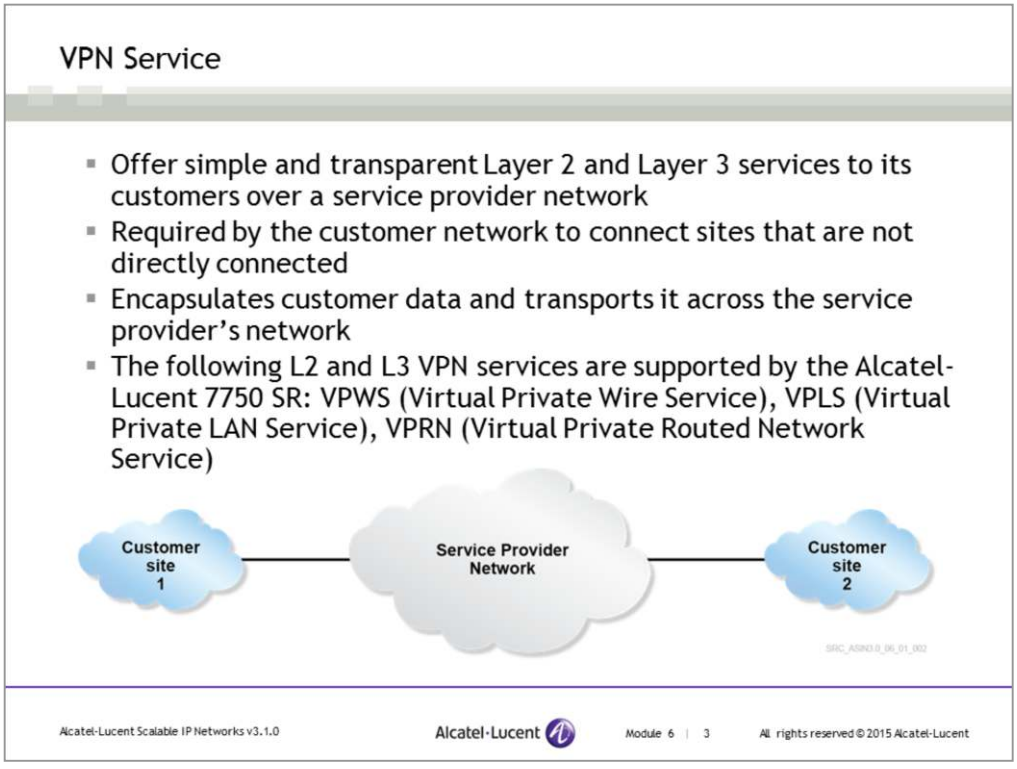
After successful completion of this module, you will be able to:

- Describe the three VPN services - VPWS, VPLS and VPRN
- Describe the different types of routers and their function in a VPN service-based network
- Describe the concept of tunneling and its role in providing VPN services
- Describe how MPLS can be used for tunneling and label switching
- Describe SAP, SDPs, and their application to VPN services

All rights reserved © 2015 Alcatel-Lucent

Alcatel-Lucent Scalable IP Networks v3.1.0 Alcatel·Lucent Module 6 | 2
All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The service provider can offer simple, transparent Layer 2 and Layer 3 VPN services to multiple customers over a single network. Three types of services are supported: VPWS, VPLS and VPRN.

Virtual Private Wire Service

Virtual Private Wire Service (VPWS) is a simple Layer 2 service that emulates a single leased line or circuit between two locations. The customer has no knowledge of the service provider network; the service acts as a simple point-to-point connection between customer sites. The VPWS can emulate an Ethernet connection (ePipe), a frame relay connection (fPipe), an ATM connection (aPipe) or a TDM circuit (cPipe). Layer 2 frames of customer data are encapsulated in MPLS labels and tunneled across the service provider network.

Virtual Private LAN Service

Virtual Private LAN Service (VPLS) is a Layer 2 multipoint service that can be used to interconnect more than two customer locations. From the customer's perspective, VPLS looks as though a simple Layer 2 LAN switch exists between different customer locations. The Ethernet frames of customer data are encapsulated in MPLS labels and tunneled across the service provider network.

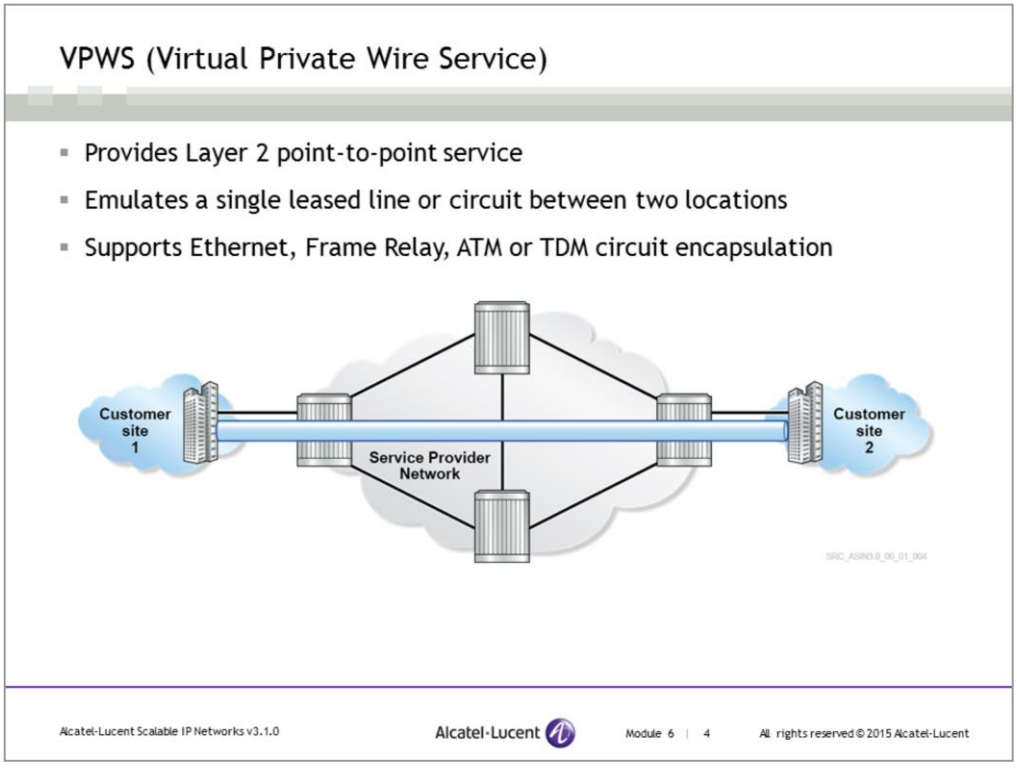
Virtual Private Routed Network

Virtual Private Routed Network (VPRN) is a Layer 3 service that makes the service provider network appear as a simple IP router that connects two or more customer locations. The VPRN allows the CE devices to exchange route information with the VPRN as if it were an IP router. The IP packets containing customer data are encapsulated in MPLS labels and tunneled across the service provider network.

VPN services are discussed in the Alcatel-Lucent Services Architecture course.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

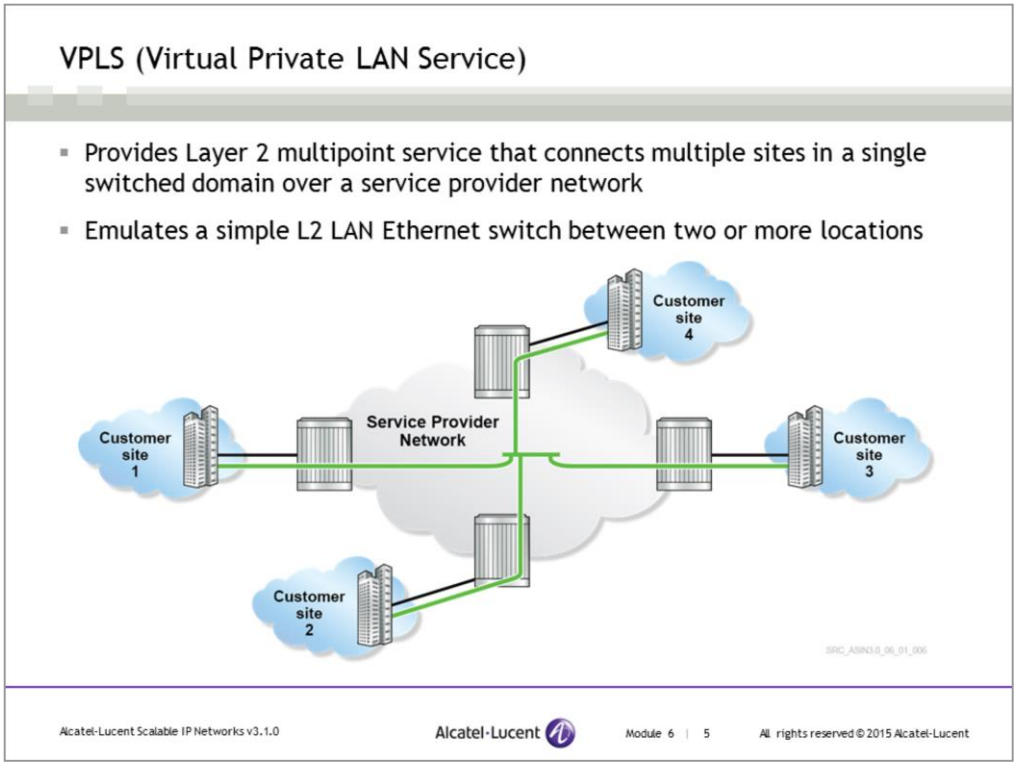


A Virtual Private Wire Service (VPWS) provides a Layer 2 point-to-point service. The VPWS encapsulates customer data and transports it across a service provider network.

The Alcatel-Lucent 7750 SR provides point-to-point Ethernet, Frame Relay, ATM (Asynchronous Transfer Mode) or TDM (Time Division Multiplexing) service.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

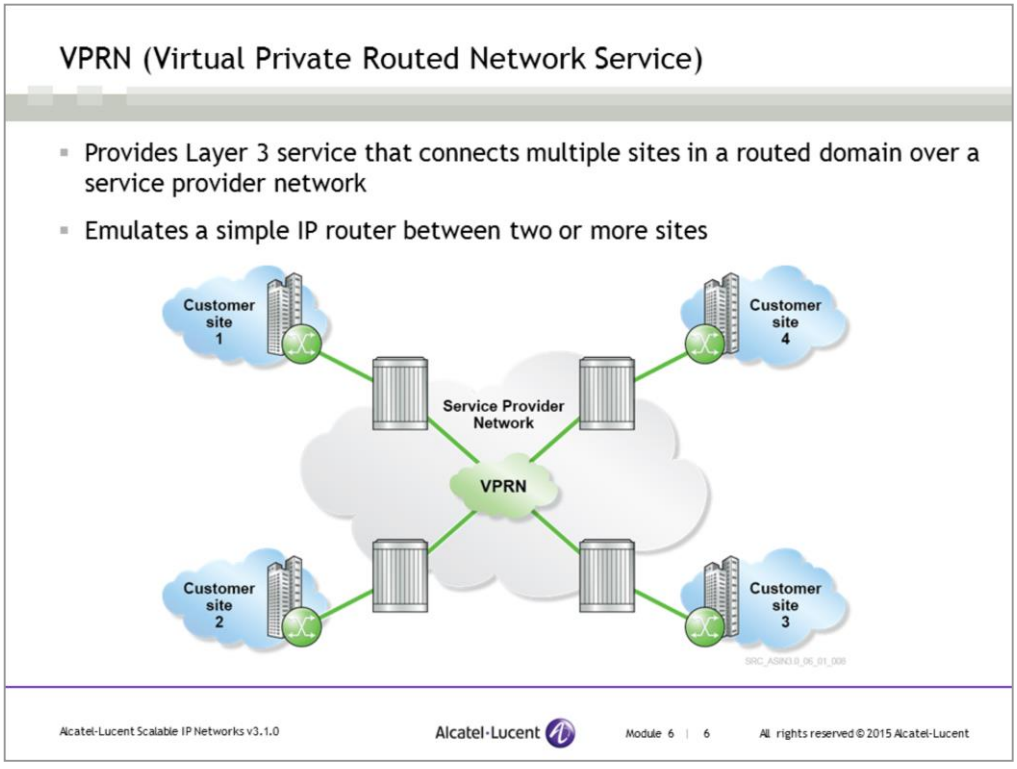


A Virtual Private LAN Service (VPLS) is a multipoint Layer 2 service that allows multiple customer sites to be connected in a single switched domain contained within a service provider network. Customer sites in the VPLS appear to be on the same LAN, even if the sites are geographically dispersed.

VPLS services switch traffic based on MAC addresses.

All rights reserved © 2015 Alcatel-Lucent

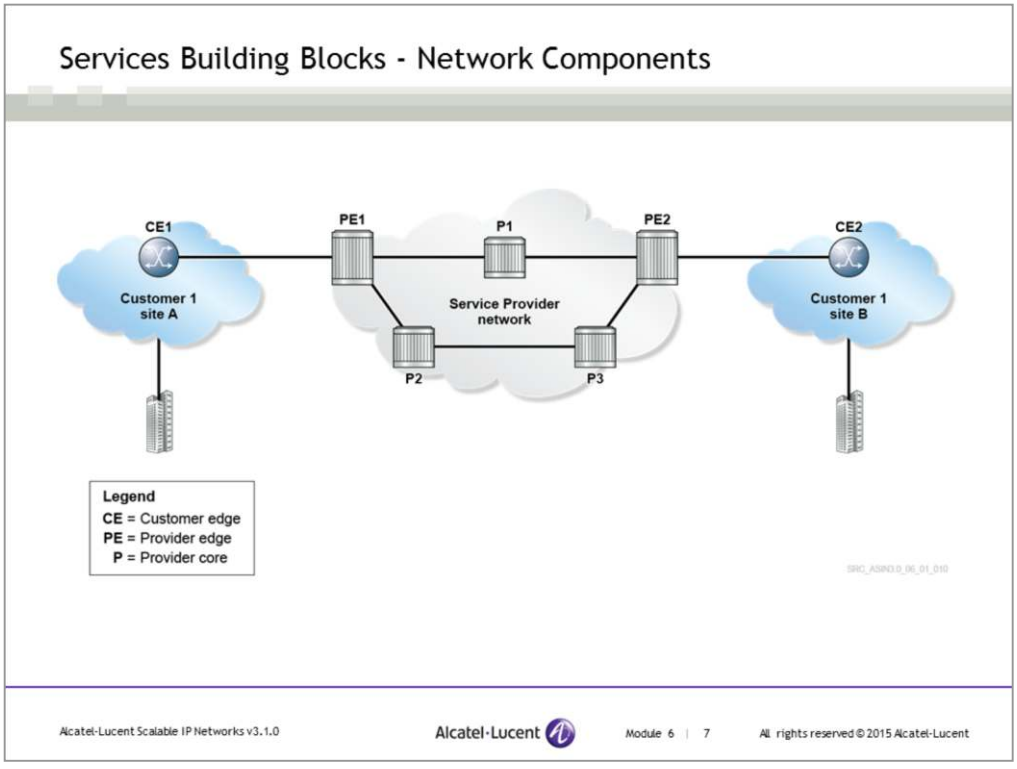
This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



IETF RFC 4364 (formerly RFC 2547bis) details a method of distributing routing information and forwarding data to provide a Layer 3 Virtual Private Network (VPN) service to end-customers. Each Virtual Private Routed Network (VPRN) consists of a set of customer sites connected to one or more PE routers. Each associated PE router maintains a separate IP forwarding table for each VPRN.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Customer edge devices

A customer edge (CE) device resides on the customer premises. The CE device provides access to the service provider network over a link to one or more provider edge (PE) routers. The end user typically owns and operates these devices. CE devices are unaware of tunneling protocols or VPN services provided by the service provider.

Provider edge devices

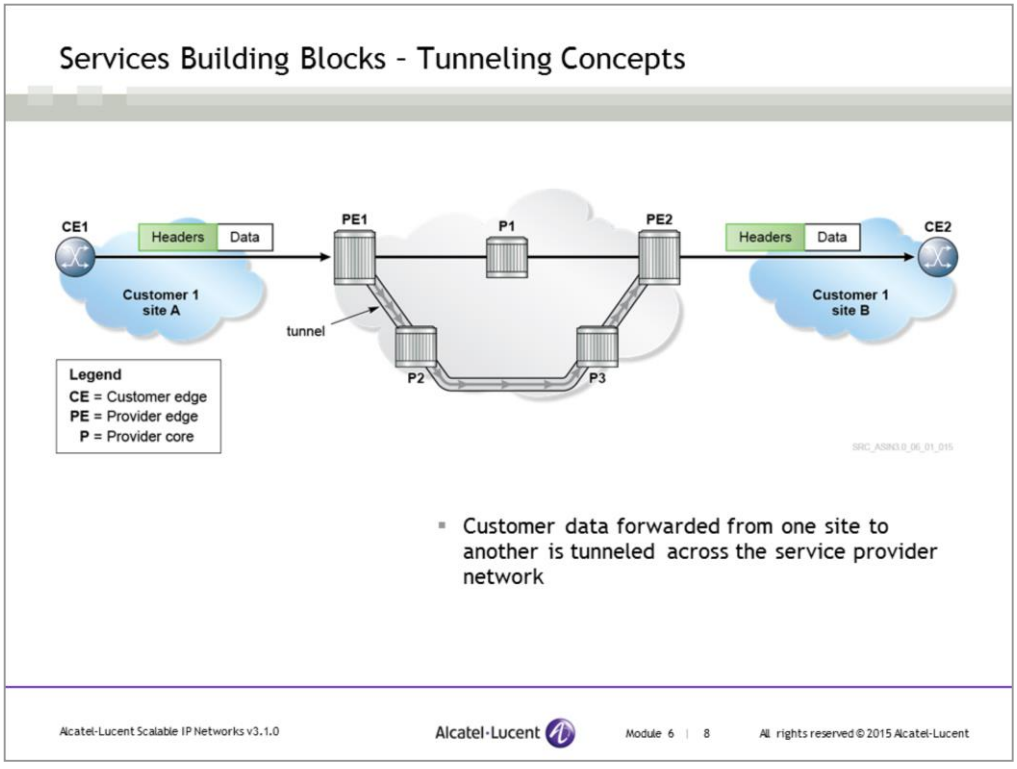
A provider edge (PE) device has at least one interface directly connected to the CE devices. In addition, a PE device usually has at least one interface that connects to the service provider core devices, or provider routers. Because the PE device must be able to connect to different CE devices over different access media, the PE device is usually able to support many different interface types. The PE device is the customer's gateway to the VPN services offered by the service provider.

Provider router

Provider (P) routers are located in the provider core network. The P router supports the service provider's bandwidth and switching requirements over a geographically dispersed area. The P router does not connect directly to the customer equipment.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



In order to provide a virtual private network (VPN) service, the service provider must encapsulate the customer data to traverse the service provider network. Depending on the nature of the VPN service, the encapsulation of the Layer 2 and Layer 3 headers may be included. Customer data must be transported without any changes across the service provider network from one customer site to another customer site. This way, the provider can attach any additional information to the original packet for forwarding inside the provider network. The provider will remove this information and forward the packet using the standard Layer 2 and Layer 3 information at the destination CE.

In order to accomplish this, an additional header is added to customer data for transport across the service provider network. Instead of routing or switching the data across the service provider's network using the customer's Layer 2 or Layer 3 headers, the data traverses the network using the header that is added at the edge of the service provider network. Therefore, customer data is effectively tunneled across the service provider network unchanged.

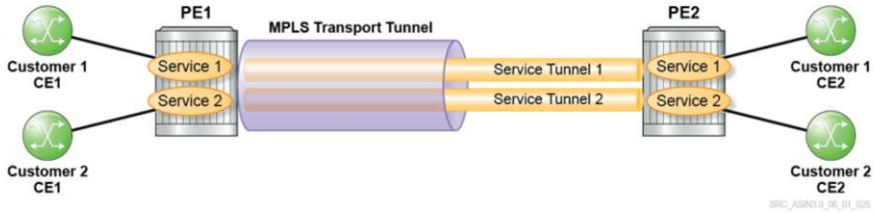
In this slide, packets from the source CE arrive at the ingress PE and are encapsulated with a tag that allows them to be forwarded through the provider network along specific paths. The forwarding path is based on this provider-created tag. The tag is removed before the packet is forwarded to the destination CE so that the original packet arrives at the destination CE unchanged.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Transport Tunnels and Service Tunnels

- MPLS (Multiprotocol Label Switching) or GRE (Generic Routing Encapsulation) transport tunnels are used to transmit customer data across the service provider network
- Service tunnels are used to identify which service or customer owns the packet
- Multiple service tunnels can be carried within a transport tunnel



All rights reserved © 2015 Alcatel-Lucent

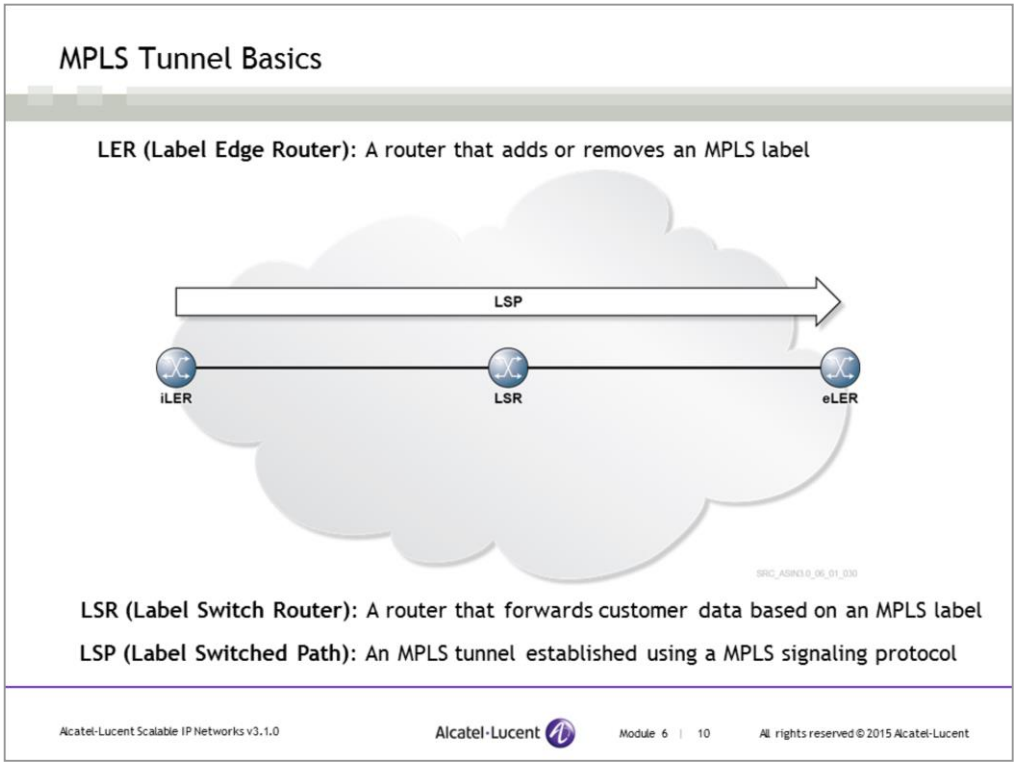
All the IP/MPLS VPN services described in section 1 use MPLS or GRE tunnels to transmit customer data across the service provider network. When MPLS is used, customer data is encapsulated with two MPLS labels; an outer transport label and an inner service label.

Alcatel-Lucent 7750 SRs are connected to physical links used to carry traffic. When a service is set up using MPLS, transport tunnel Label Swiched Paths (LSPs) are set up between provider edge, or PE, routers. Each service or customer sends traffic through a service tunnel within the transport tunnel LSP. Transport tunnel LSPs are identified by MPLS labels that are swapped at each intermediate router, also known as a transit Label Switch Router (LSR), along the LSP from the ingress to the egress of the MPLS network.

The service label, or inner label, is used to identify which service or customer owns the packet. In the identification process, the label is attached at the ingress point and does not change value as the packet travels from ingress to egress.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



The purpose of MPLS is to provide a tunneling service to forward customer packets across the provider network by adding a special header called a *label*. The label is simply an additional header added to packets coming into the provider network.

In an MPLS network, routers are categorized as Label Edge Routers (LERs) or Label Switch Routers (LSRs).

The LERs are the endpoints of the MPLS tunnels, known as Label Switched Paths (LSPs), and are normally at the edge of the network.

The ingress LER (iLER) is the starting point of the LSP, or the start of the tunnel. The egress LER (eLER) is the termination point of the LSP, or the end of the tunnel.

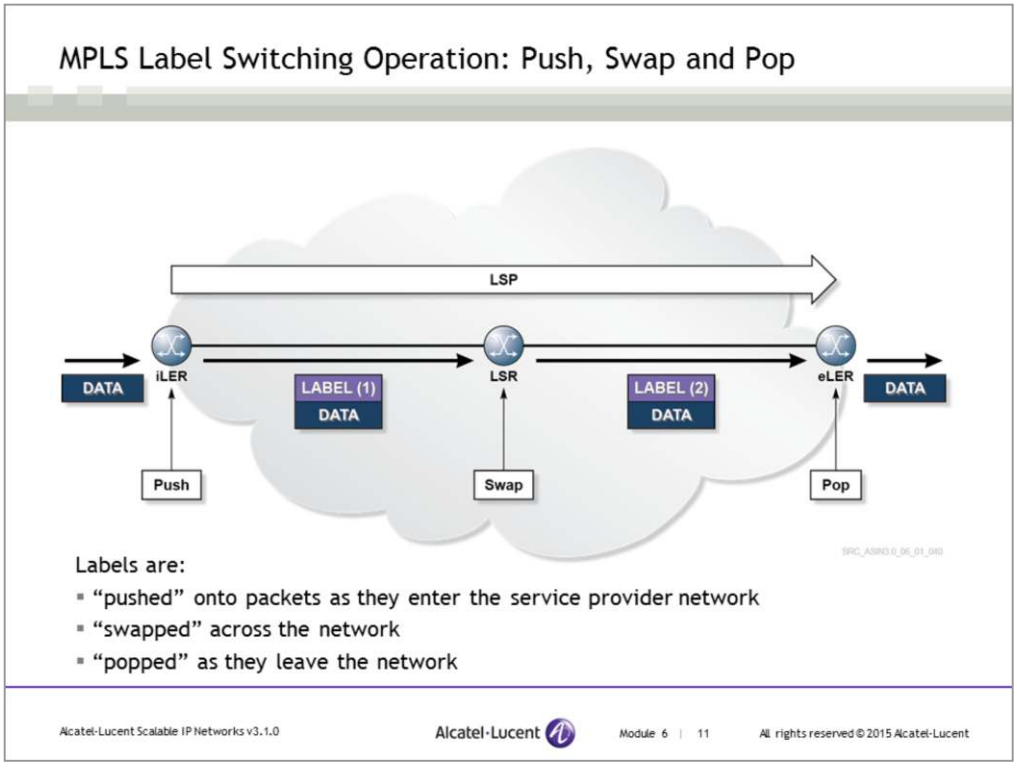
The LSPs are set up using an MPLS signaling protocol, such as LDP (Label Distribution Protocol) or RSVP-TE (Resource Reservation Protocol with Traffic Engineering extensions). RSVP and LDP are covered in more detail in the Alcatel-Lucent MPLS course.

The LSRs are at the core of the network and provide connectivity between the LERs.

The MPLS-enabled routers (LERs and LSRs) use a signaling protocol to distribute labels across the network. These labels are used to make the forwarding decision for incoming traffic, rather than the IP address. This turns the Layer 3 routed network into a switched network.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Before an LSP (Label Switched Path) is established, labels must be distributed using MPLS signaling protocols. LDP and RSVP-TE are examples of MPLS signaling protocols.

This slide illustrates the forwarding process of an MPLS labeled packet.

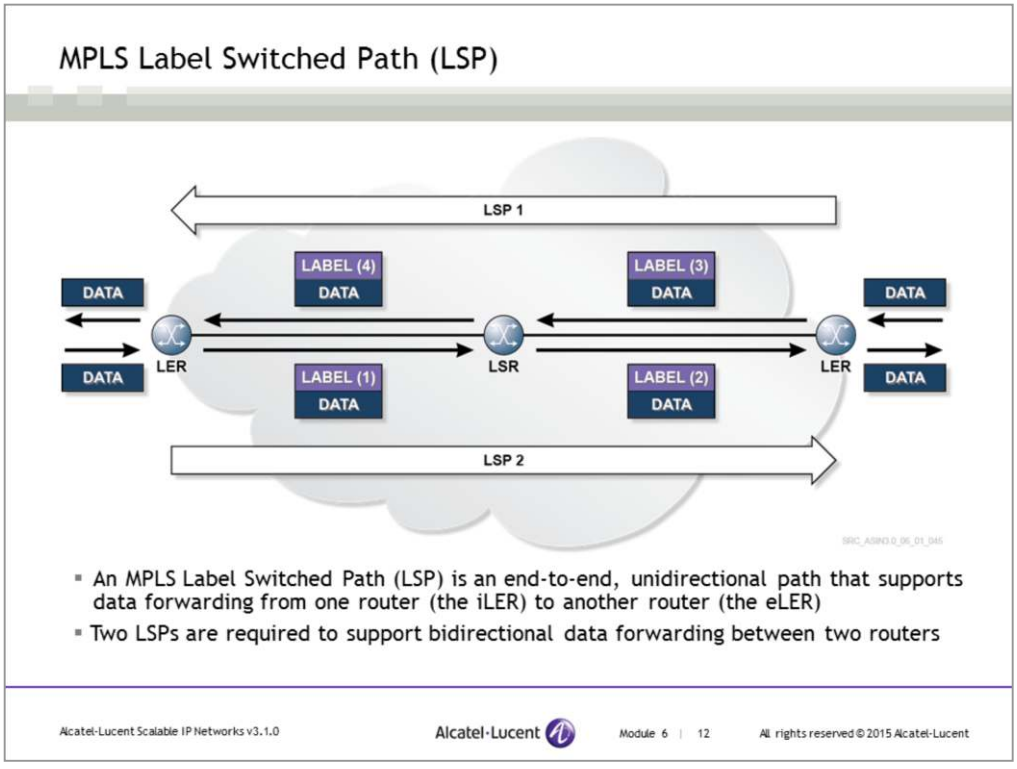
A label is added to the "unlabeled" packet by an LER at the ingress to the service provider core network. This is called a Push operation.

The LSR checks the incoming label against its Label Forwarding Information Base (LFIB) to find the interface and outgoing label needed to forward the packet to the next-hop. This is called a Swap Operation.

The LER at the egress of the service provider core network strips the incoming label and sends the packet again as "unlabeled" to the customer network.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A Label Switched Path (LSP) can be defined as a sequence of labels and label actions performed on MPLS routers to forward data packets from point A to point B, using label switching.

A Label Switched Path always starts from an iLER and ends at an eLER. An LSP is thus an end-to-end, unidirectional path that carries traffic from one router to another.

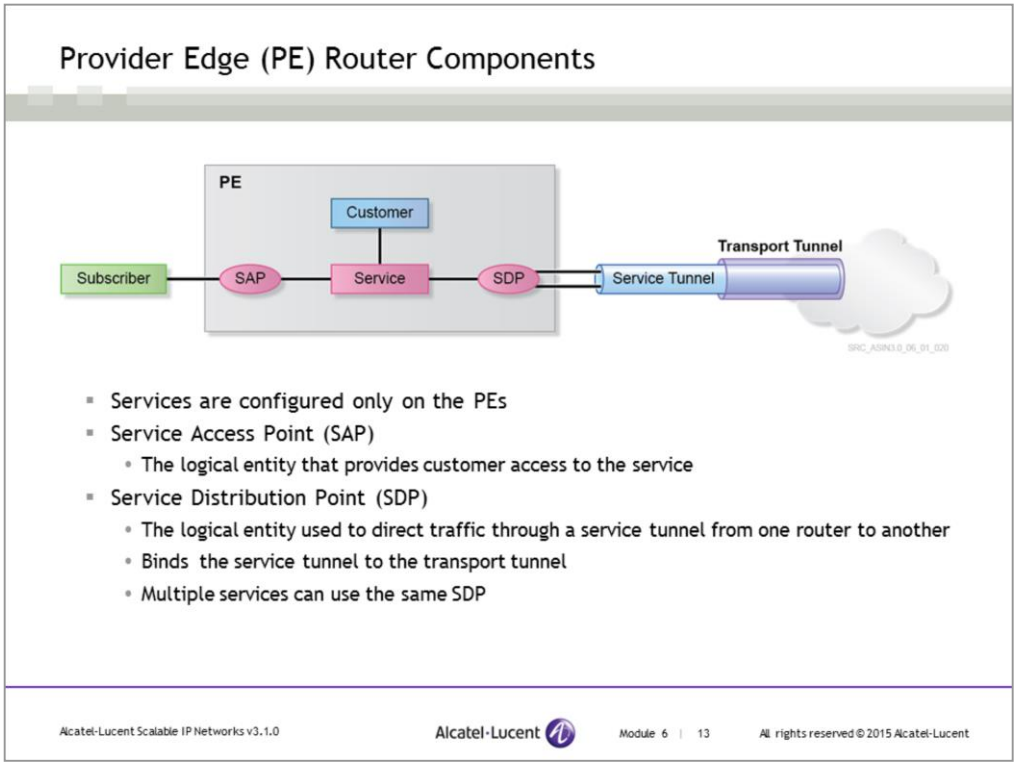
In the above slide, traffic flows from right-to-left for LSP 1 and traffic flows from left-to-right for LSP 2.

The encapsulation and forwarding of packets using labels is also referred to as tunneling. Therefore, LSPs are often called tunnels.

Tunnels must be established prior to the arrival of data packets.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A PE router provides a Service Access Point (SAP) to a subscriber/customer that connects customers to an individual service. The PE connects to a Service Distribution Point (SDP) that provides tunneling services through the provider's core network.

The terms customers and subscribers are used synonymously.

The customer ID is assigned when the customer account is created. This allows a provider to uniquely identify services configured for a particular customer through its network.

To provision a service, a customer ID must be associated with the service at the time of service creation.

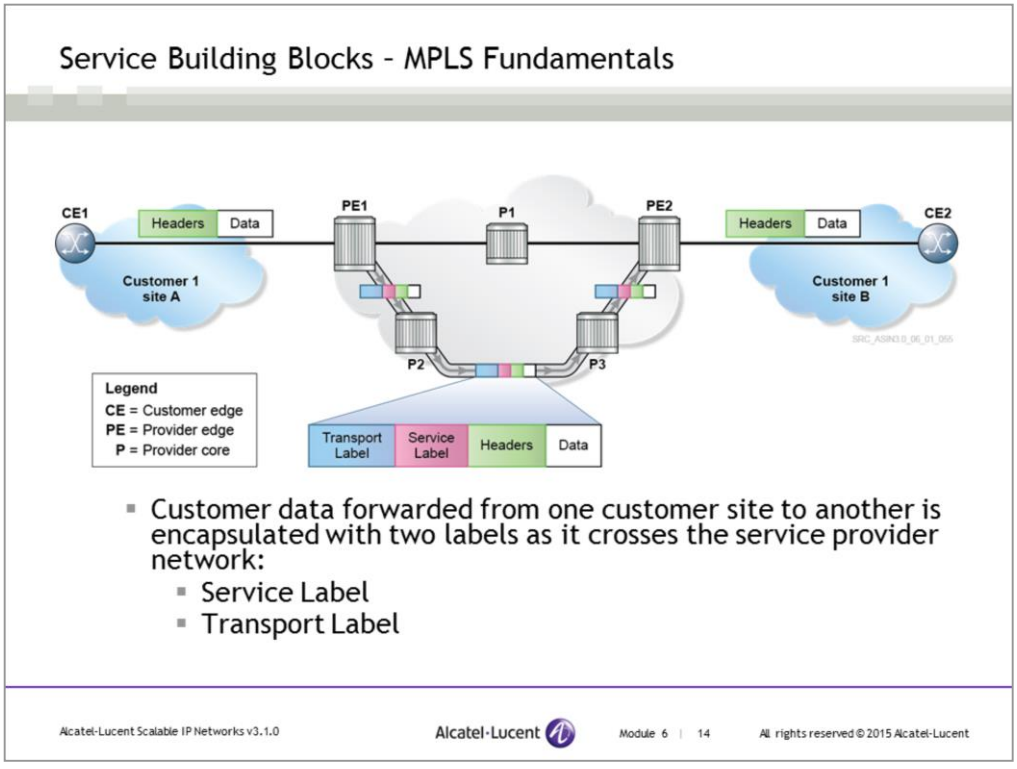
P and CE routers are not aware of the services, and they do not need to configure any service components, such as SAP or SDP.

An SAP is a logical entity that serves as the customer's point of access into a service. Each service is configured with at least one SAP. An SAP ID is locally unique. This means that the same SAP ID value can be used on another service router.

An SDP is a logical entity that directs traffic from one router to another through a unidirectional service tunnel. The SDP terminates at the far-end router, which directs packets to the egress SAP on that router. An SDP ID is locally unique. This means that the same SDP ID can be used on another service router. An SDP is not specific to one service. Many services can use the same SDP.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



As a customer data packet is forwarded from one customer site to another customer site, it is encapsulated with two labels as it crosses the service provider network.

1. Service Label
   This label is carried transparently across the service provider network and is used at the far end PE to identify the service that the packet is destined for.
2. Transport Label
   This label is modified across the service provider network and is used to deliver packets to the far end PE.

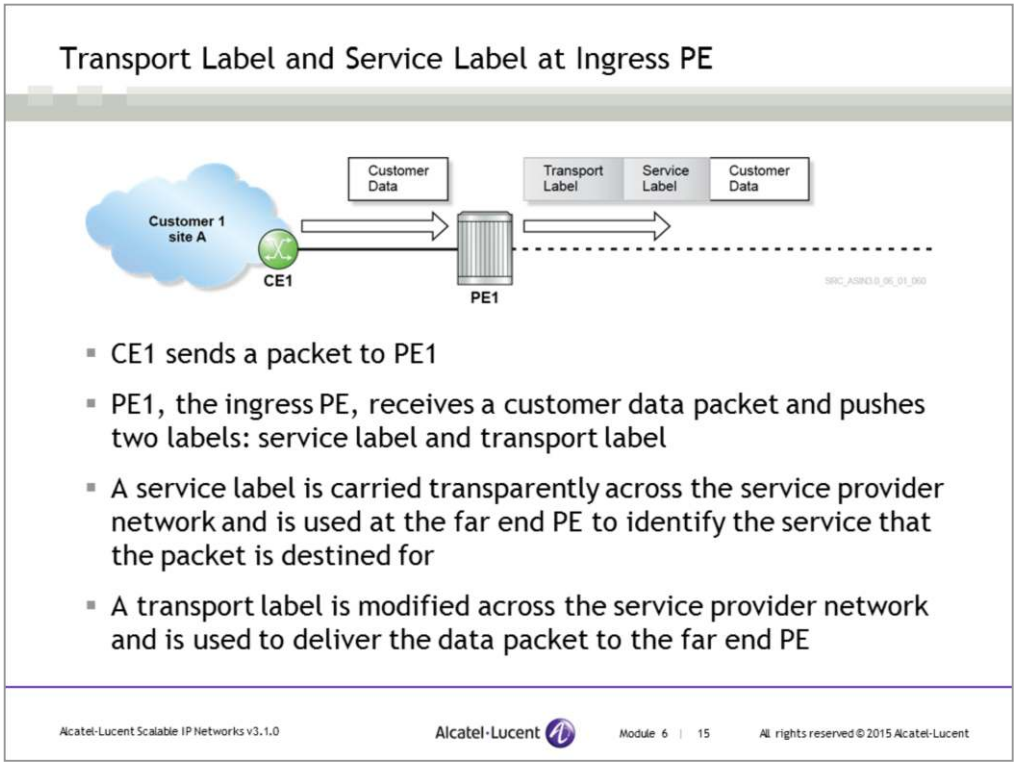
Packet walkthrough

In this slide, CE1 sends a data frame towards CE2. On an Ethernet interface, this is a normal IP datagram encapsulated in Ethernet. CE1 is not aware of the MPLS LSP that originates on PE1. The packet sent from CE1 to PE1 is unlabeled because the packet does not contain an MPLS label.

1. When the packet reaches PE1, two labels, a service label and a transport label, are applied to the frame. The transport label corresponds to the LSP that ends on PE2. The service label identifies the service that the packet is destined for. The labeled MPLS packet is then sent along the LSP to P2.
2. P2 processes the MPLS packet and checks its MPLS table to perform a label swapping operation. It reads the transport label in the packet, performs a table lookup, switches the packet out of the appropriate interface to P3, and applies a new transport label.
3. P3 performs a similar label swap operation and switches the MPLS packet out from its interface to PE2 with a new transport label.
4. When PE2 receives the labeled packet, PE2 performs a lookup on the received transport label. Because PE2 is an edge router directly-connected to CE2, PE2 strips both the transport label and service label and forwards the unlabeled packet to CE2. As with CE1, CE2 is totally unaware of the LSP through the provider core. CE2 receives the same customer data as though CE1 and CE2 were directly-connected.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



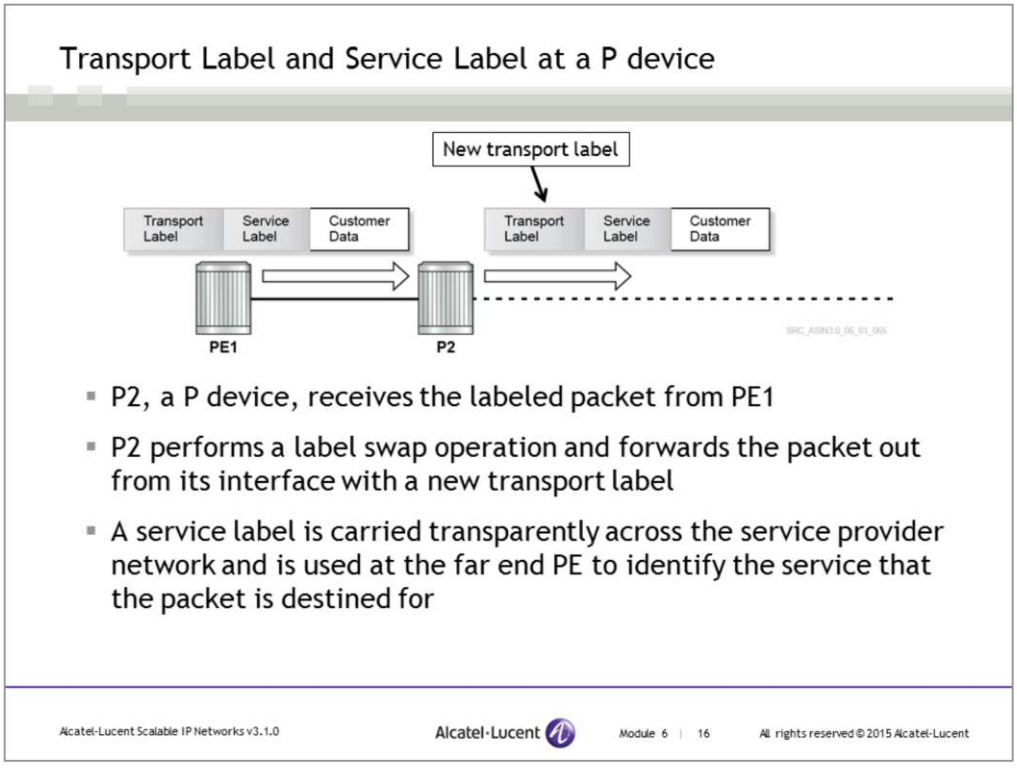
The ingress PE receives customer data on a Service Access Point (SAP) associated with a specific service. The SAP may be a port, a port with a specific Virtual Local Area Network (VLAN) tag in the case of an Ethernet port, or a port with a specific circuit ID in the case of ATM or frame relay. The customer data is then encapsulated with a service label by the ingress PE. Because many services may be configured on the PE, the service label identifies the specific service that the data belongs to.

After the data is encapsulated with the service label (also called inner label), the data must be forwarded over the correct Service Distribution Point (SDP) that is defined by the service. A second label, the transport label (also called outer label), is added to the data. This label identifies the LSP that will be used to transport the MPLS packets to the far end of the tunnel, the egress PE device. The data is label-switched along the LSP using this outer label.

Note that CE devices are not aware of SDPs and SAPs.

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



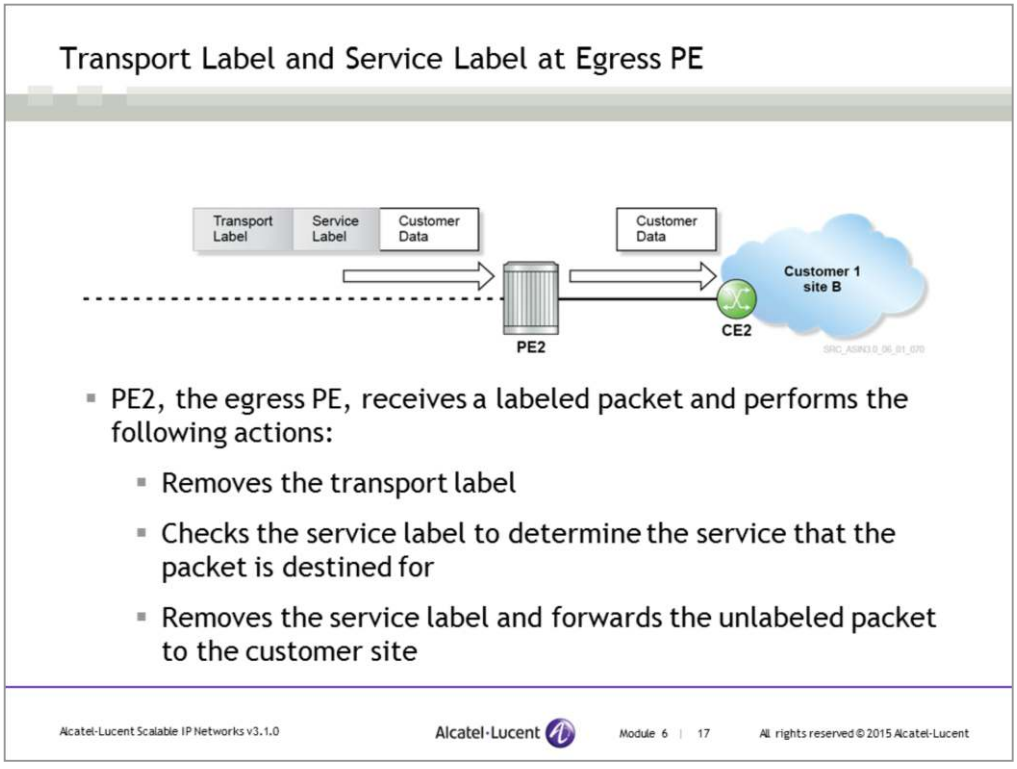
The P device receives the customer data packet encapsulated with two labels: a transport label and a service label.

As the packet traverses the P devices the transport label is swapped, while the service label remains unchanged.

Note that P routers are not aware of SDPs and SAPs.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

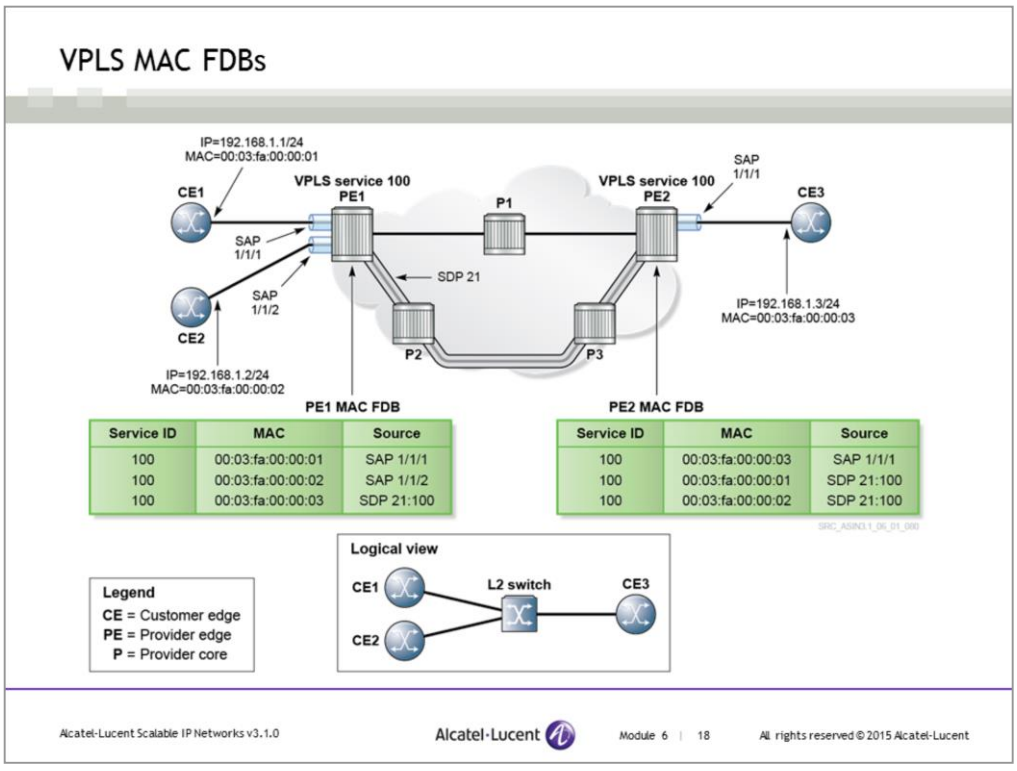


When the egress PE receives the MPLS packets, it removes the MPLS-encapsulated data from the SDP. The outer transport label is removed. The inner service label is used to identify the service that the data belongs to. After the labels are removed, the data is transmitted on the appropriate SAP for the service. In other words, the service label is used to de-multiplex the data from the SDP to the appropriate service.

CE devices are not aware of SDPs and SAPs. The CE devices receive an unlabeled packet from the egress PE device.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

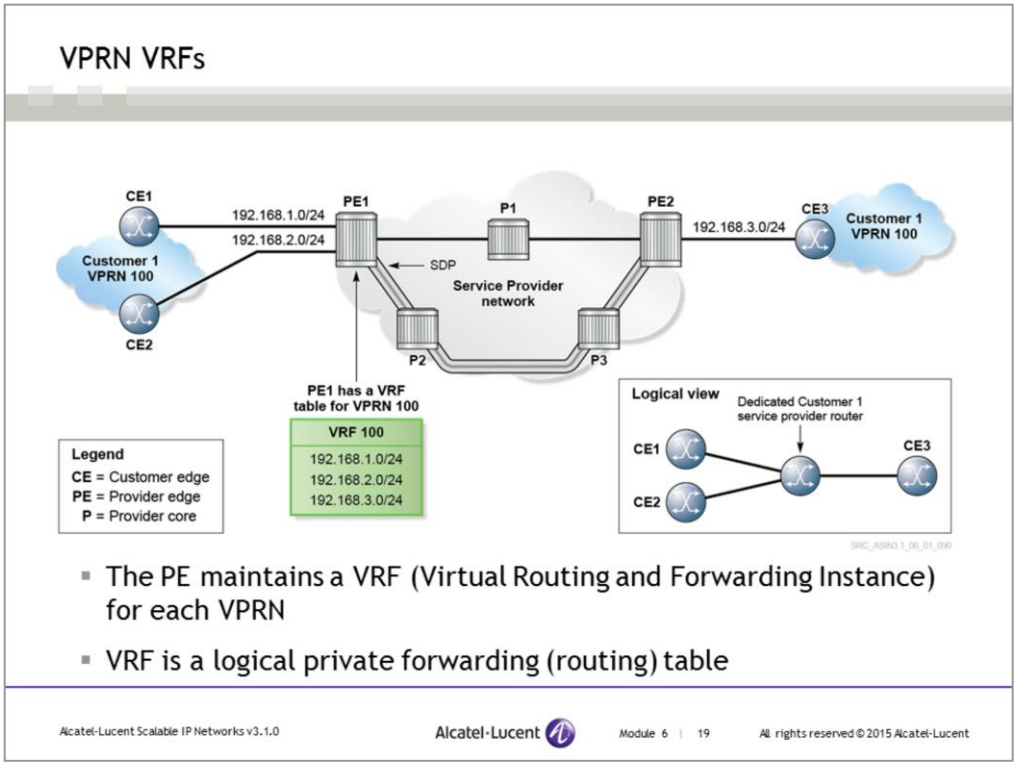


Because a VPLS emulates a switched Ethernet service, a MAC address forwarding database (FDB) must be maintained for each VPLS. When a unicast frame with an unknown source address arrives on an SAP or an SDP, the VPLS learns the address in the same way that an Ethernet switch learns a MAC address on its ports. Though the VPLS FDB associates MAC addresses with SAPs and SDPs, it is otherwise similar to an Ethernet switch.

When an Ethernet frame arrives on an SAP or an SDP, a lookup is performed in the FDB for the destination address. If there is an entry for the address, the frame is forwarded to the appropriate SAP or SDP. If there is no entry for the address, the frame is flooded to all other SAPs and SDPs, which is similar to the flooding of an unknown frame on an Ethernet switch.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



A VPRN is a class of VPN that allows the connection of multiple sites in a routed domain over a service provider IP/MPLS network. VPRN is a Layer 3 service (as opposed to VPWS and VPLS, which are Layer 2 services).

From the customer's perspective, all of the sites appear to be connected to a private, routed network administered by the service provider for that customer only. Each PE router providing VPRN services maintains a separate IP forwarding table for each VPRN. Each customer of the service provider has their own private IP address space and, therefore, may have overlapping IP addresses.

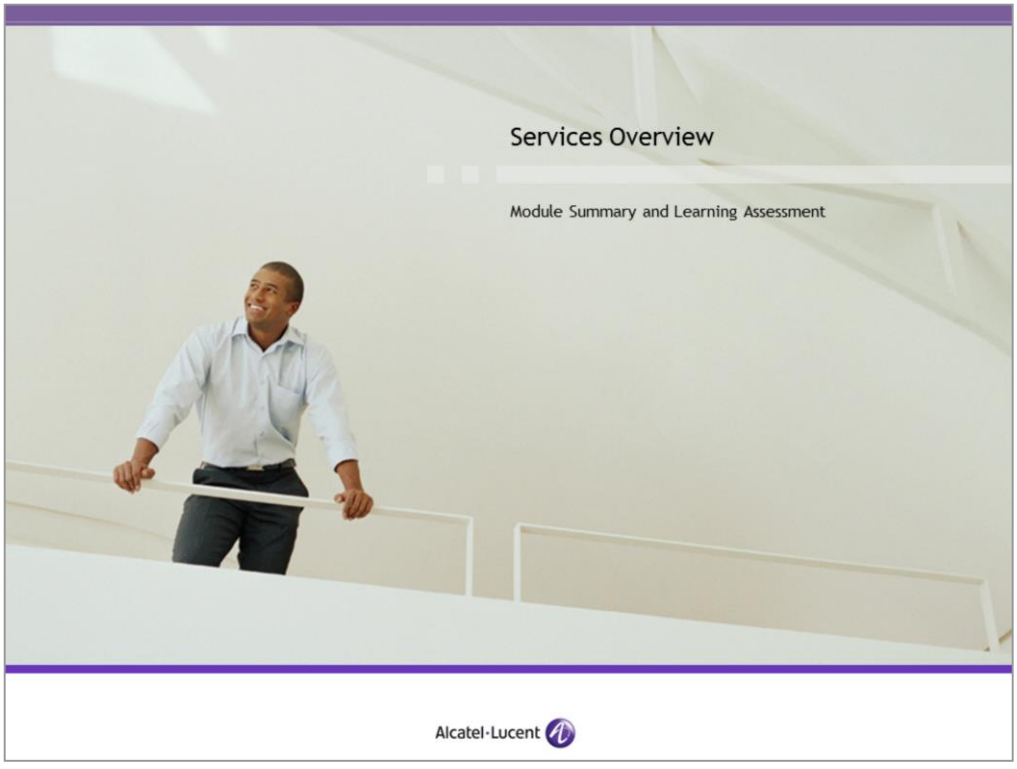
The VPRN service uses VPN Routing and Forwarding Instances (VRFs) within the PE device to maintain forwarding information on a per-customer basis. A VRF is a logical private forwarding (routing) table that securely isolates the routing information of one customer from the next customer, and also from the routes of the provider core network. Each PE maintains multiple separate VRFs that are based on the number of distinct VPRN services that the PE supports.

Each CE router becomes a routing peer of the provider PE router that it is directly connected to. Routes are exchanged between the CE and the PE routers. The PE devices in a VPRN service exchange routes with each other so that the routes can be transmitted to the remote CE devices of the customer.

The transport of customer data is similar to a VPWS or VPLS, except that the Layer 2 headers are removed and the IP datagrams are encapsulated with the MPLS headers. Customer data arrives at a VPRN SAP, is encapsulated with an inner service label and an outer transport label, and is then carried across the network using MPLS.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

Module Summary

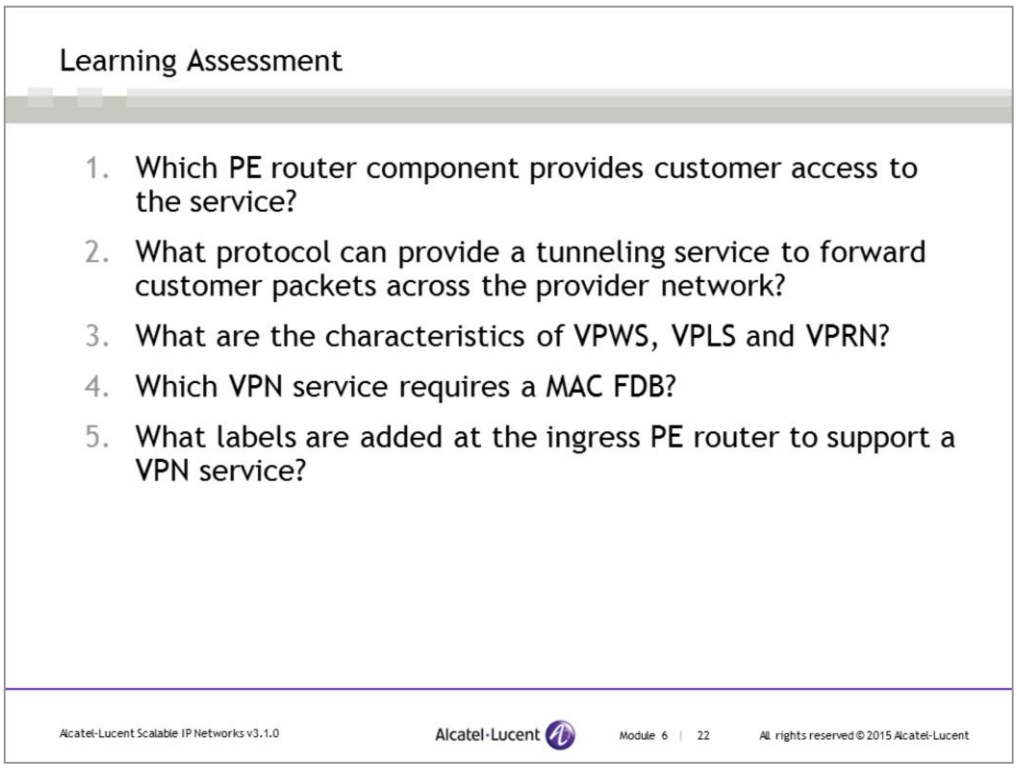
After successful completion of this module, you should be able to:

- Describe the three major VPN services - VPWS, VPLS and VPRN
- Describe the different types of routers and their function in a VPN service-based network
- Describe the concept of tunneling and its role in providing VPN services
- Describe how MPLS can be used for tunneling and label switching
- Describe SAPs and SDPs, and their application to VPN services

All rights reserved © 2015 Alcatel-Lucent

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



Learning Assessment Answers

1. Which PE router component provides customer access to the service?

Service Access Point (SAP)

2. What protocol can provide a tunneling service to forward customer packets across the provider network?

MPLS

3. What are the characteristics of VPWS, VPLS and VPRN?

VPWS – provides L2 point-to-point service and emulates a single leased line or circuit between two locations

VPLS – provides L2 point-to-multipoint service and emulates a simple L2 LAN switch between two or more locations

VPRN – provides L3 service and emulates a simple IP router between two or more sites

4. Which VPN service requires a MAC FDB?

VPLS because it emulates a switched Ethernet service

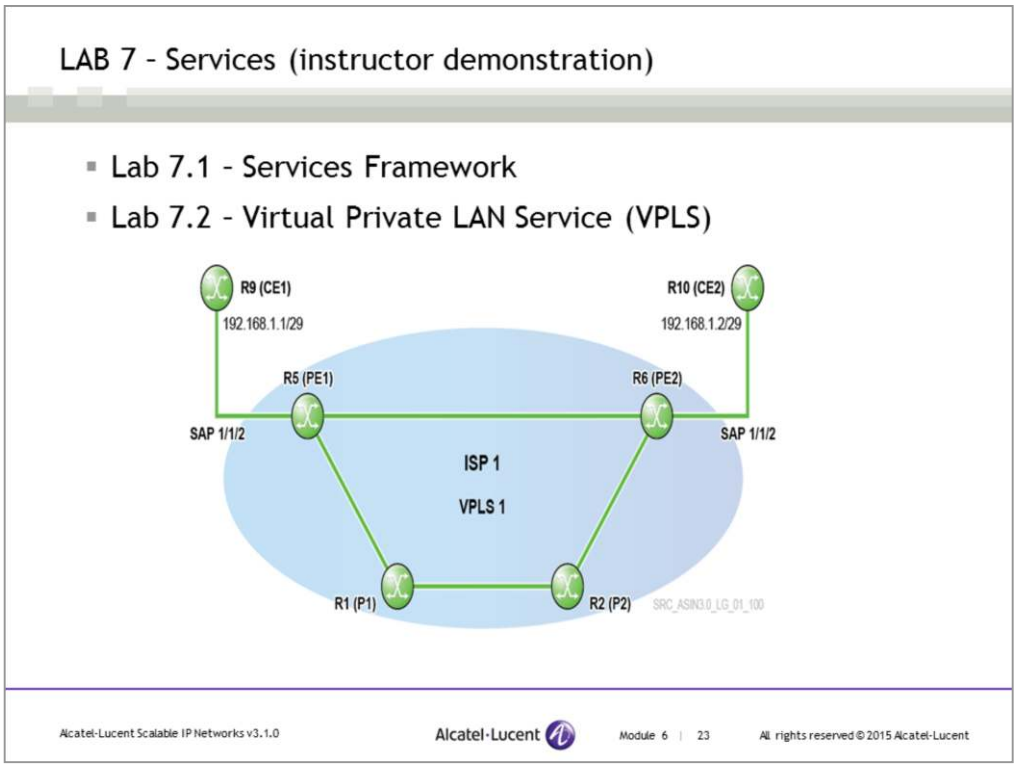
5. What labels are added at the ingress PE router to support a VPN service?

A service label to determine what service the frame belongs to

A transport label to transport the MPLS packets to the egress PE

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT



See the *Alcatel-Lucent Scalable IP Networks Lab Guide*.

 All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT

All rights reserved © 2015 Alcatel-Lucent

This Nokia Scalable IP Networks Courseware v3.1 is for the exclusive use of Raul NAGY - ALCATEL-LUCENT