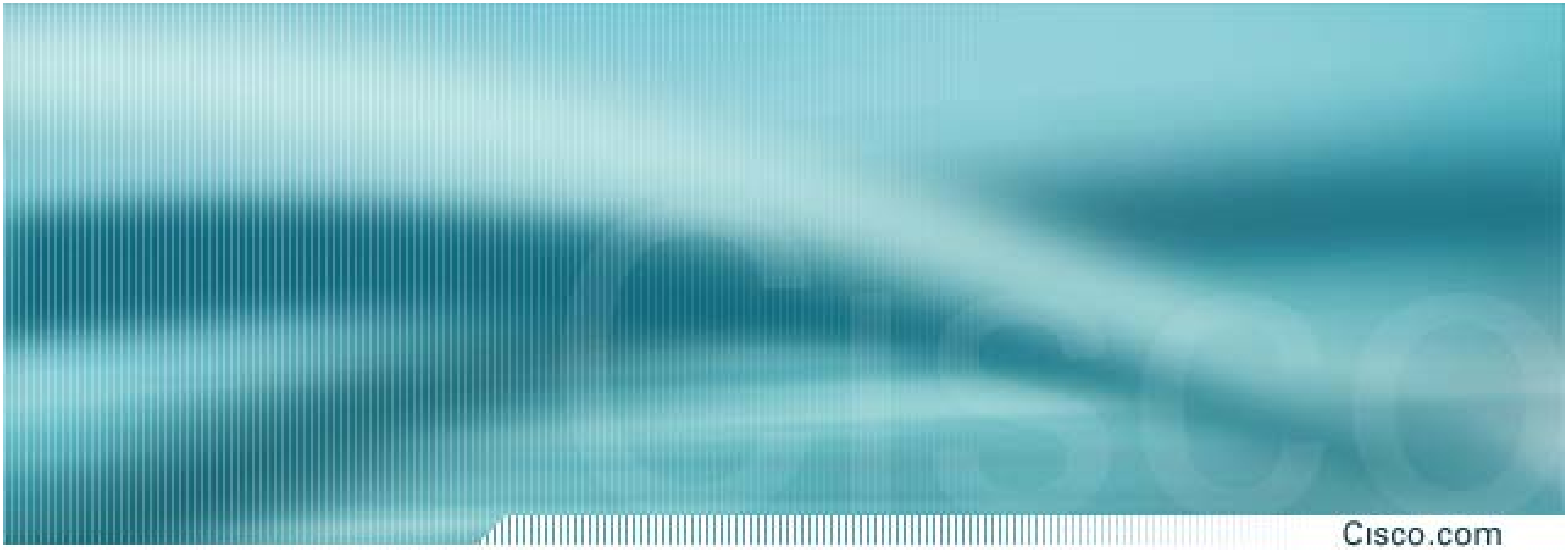
NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Cisco Systems



CCIE Power Session

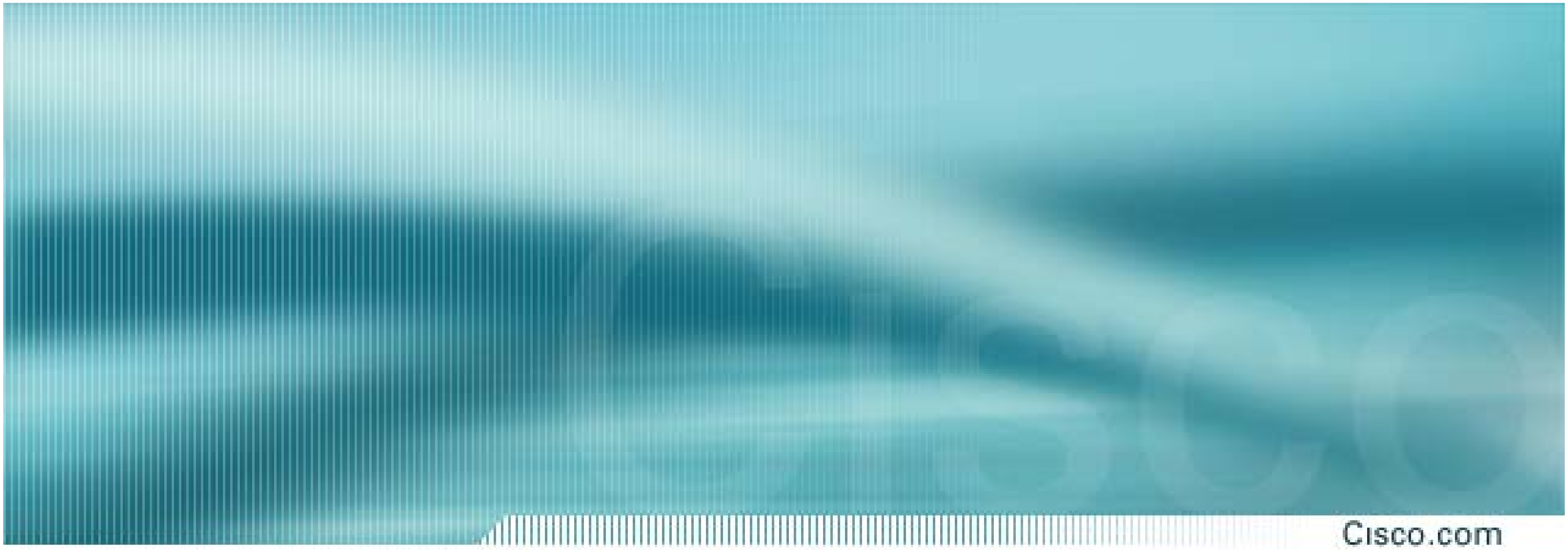
Session PWR-5014

Power Session Topics

Session 1	CCIE Roadmap/Exam Basics
Session 2	Spanning Tree/Multi-Layer Switching/DLSWoE
Session 3	QOS/IP Routing Concepts
Session 4	IP Routing OSPF
Session 5	IP Routing BGP
Session 6	Multicast/ATM/Security
Session 7	ISDN and Dial Features
Session 8	Preparation/Q&A

Content Note

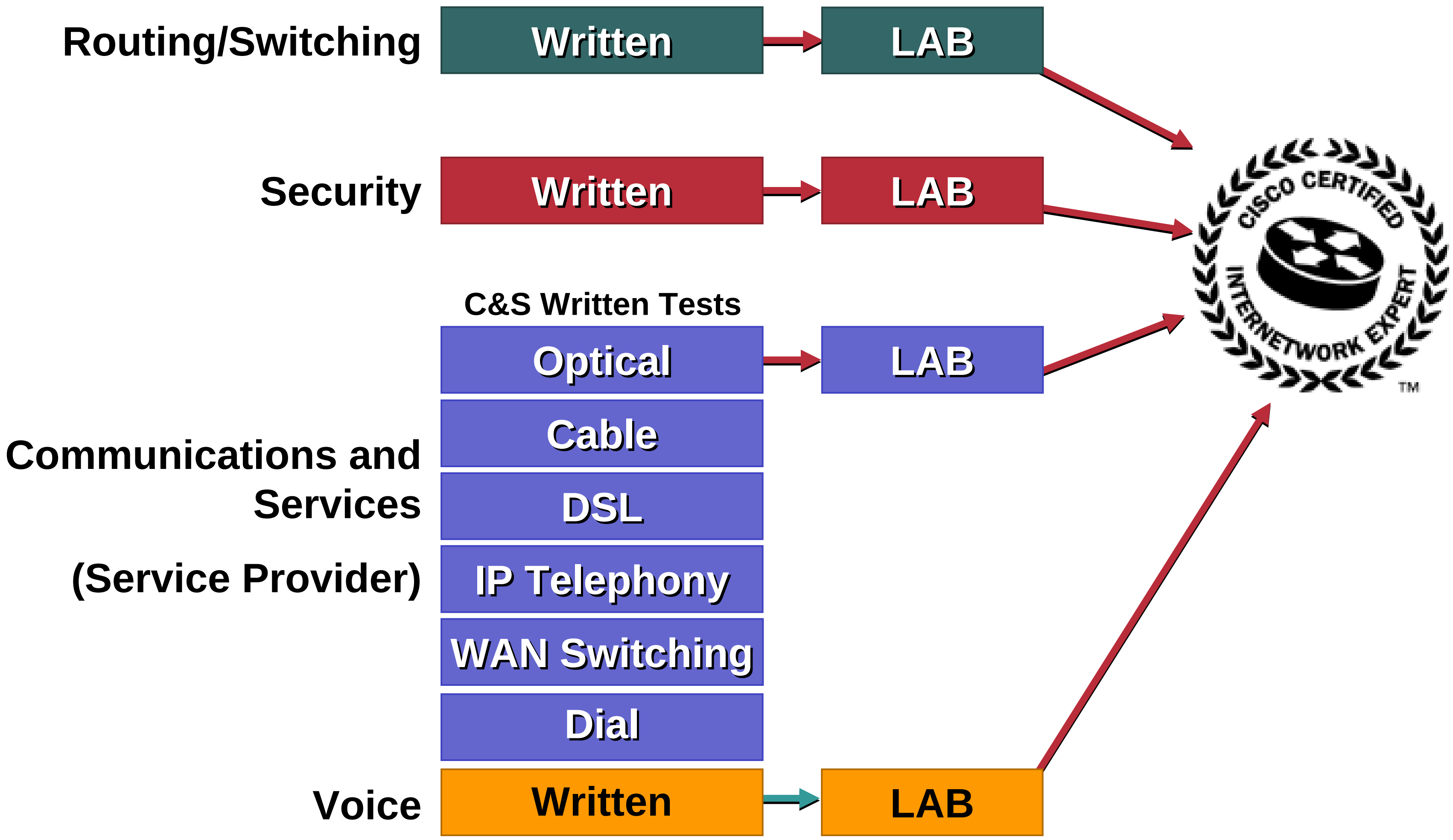
- Not all the topics discussed today appear on every exam
- For time reasons, we’re unable to discuss every feature and topic possible on the exam



Session 1

CCIE Exam and Configuration Fundamentals

CCIE Program



CCIE Program (Cont.)

- **Each exam track has a separate qualification exam (or set of qualification exams) and a lab exam**
- **Not all exams are available at all sites**
- **There are more than 9500 CCIE's worldwide**

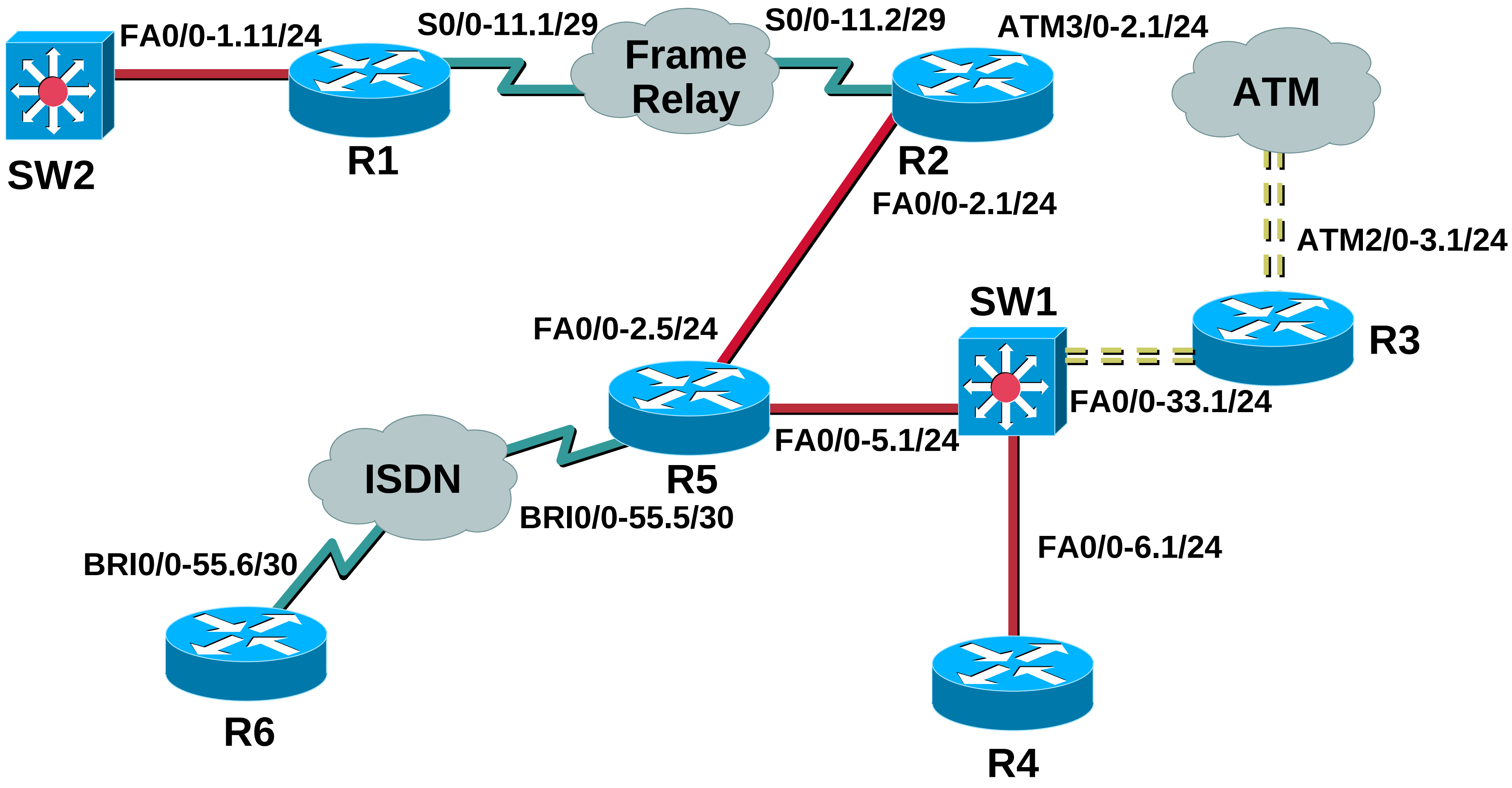
Lab Exam Format

- Candidate builds a network to a supplied specification
- The exam is graded after the candidate is finished for the day
- R/S Exam results will be available on the web to the candidate within 24 hours
- Security, C&S and Voice will be emailed within 48 hours

Lab Exam Format

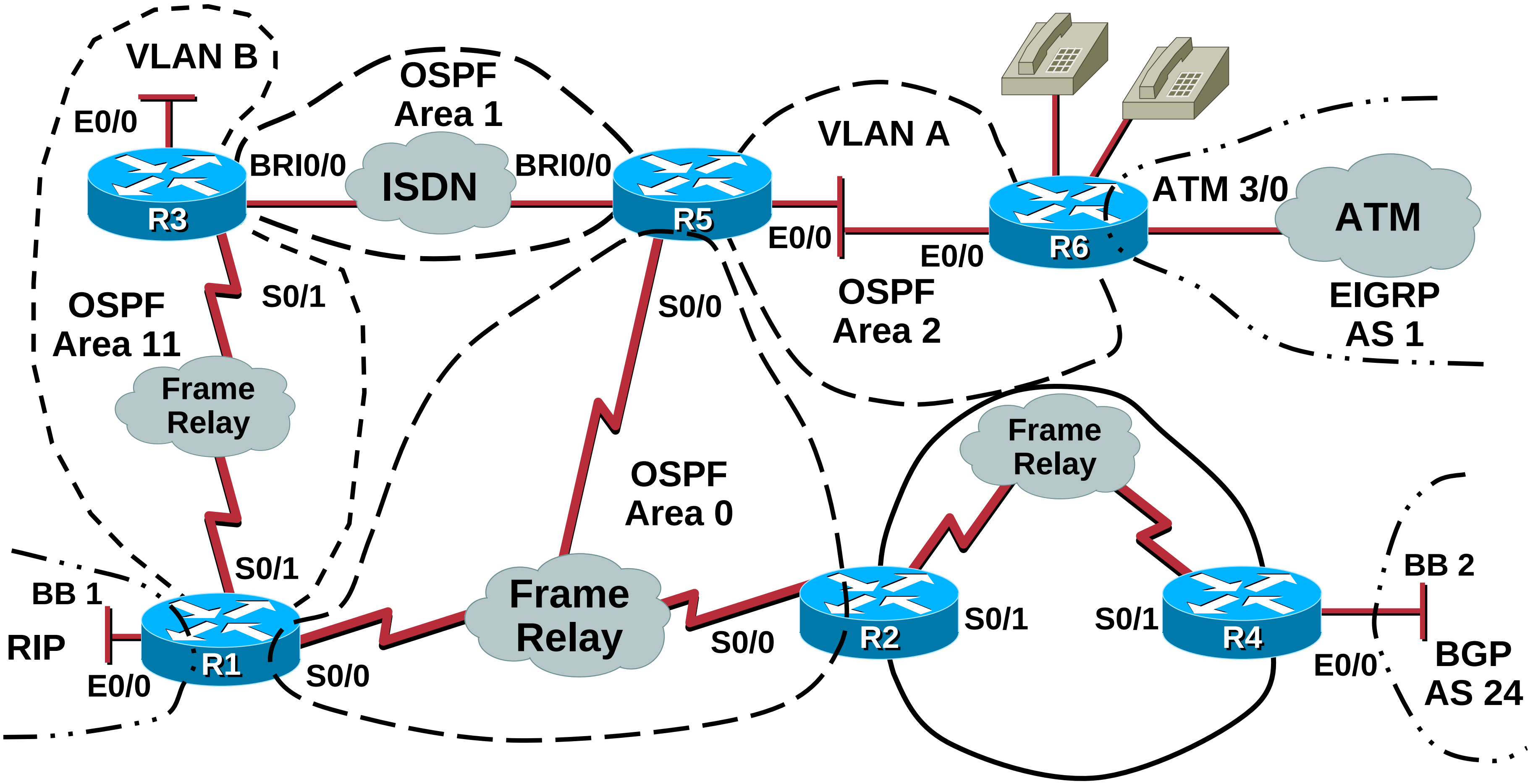
- The “network specification” is a series of questions
- Point values for each question are shown on the exam
- The questions can be done in any order, but some questions depend on the completion of previous parts of the network

Sample Topology



Sample Protocol Boundaries Diagram

Cisco.com



Sample Question

- **2.5 RIP**

  Configure RIP on R1, R2, and R5

  Redistribute between RIP and OSPF on R5

  The class B loopback on R1 should not appear in the OSPF domain

  All other routes should be visible on all routers

Scoring

2 Points

Grading the Exam

- Partial marks are not awarded for questions
- Some questions have multiple solutions
- Points are awarded for working solutions only

Standard Restrictions

- **Unless a question says so, you are not permitted to use**:**
  - **Static routes (of any kind)**
  - **Default routes**
  - ****Dynamic routes to null are permitted**

Test Philosophy

- The Routing and Switching exam tests your ability to apply configuration knowledge and skill to new situations; it is not a design test, nor is it always a test of “best practices” for use in the field

Lab Layout

Racks Are Fully Cabled

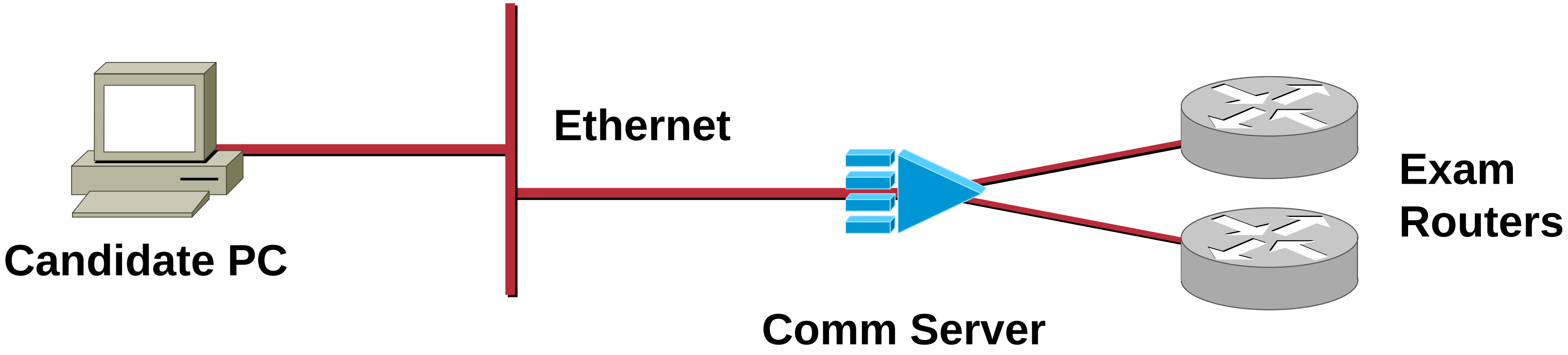
Candidates Do Not Have to Touch Racks

Lab Layout (Cont.)

- **Each candidate has his/her own PC and rack of equipment**
- **Check the CCIE web page for the latest equipment list**

Rack Access

Rack Connection Method:



Ethernet

Candidate PC

Exam Routers

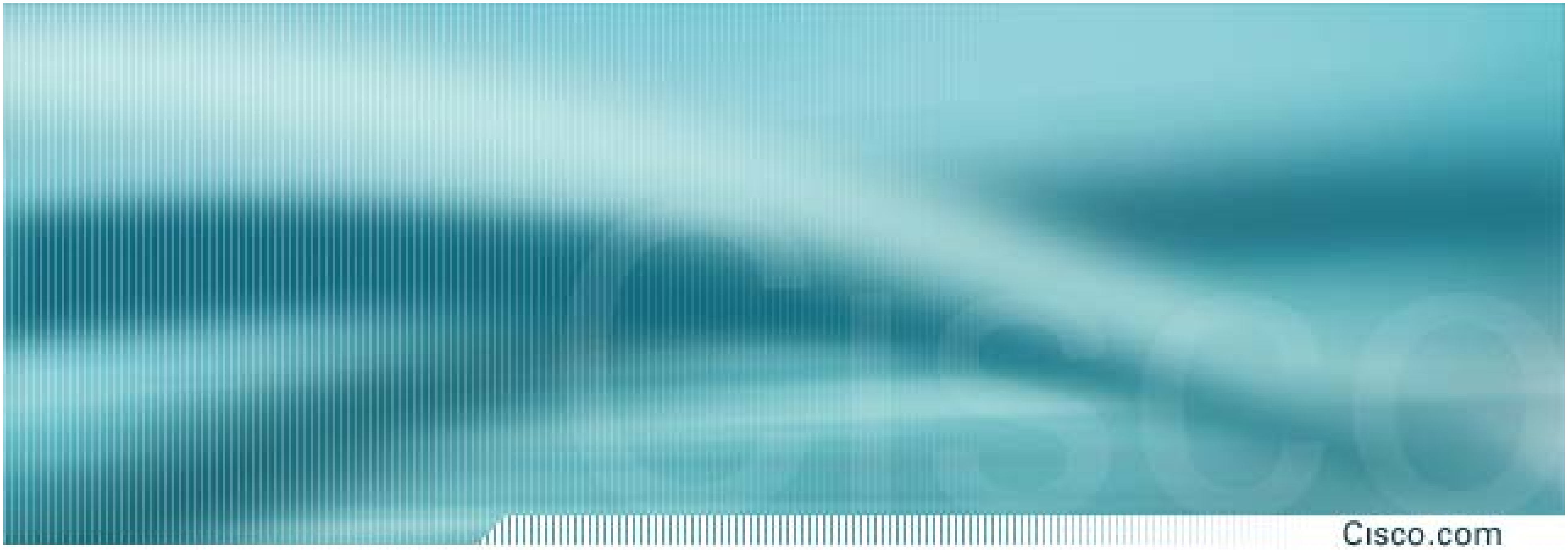
Comm Server

Passwords

- **All routers and switches have a startup configuration: hostnames, passwords, line setup, and IP addresses for primary interfaces are already configured; since all tests require the router to be accessible via the VTY and AUX ports, do not change these established configs**
- **Know the password recovery procedures for the devices in the equipment list**

Cisco.com

Questions?



Session 2

Spanning Tree

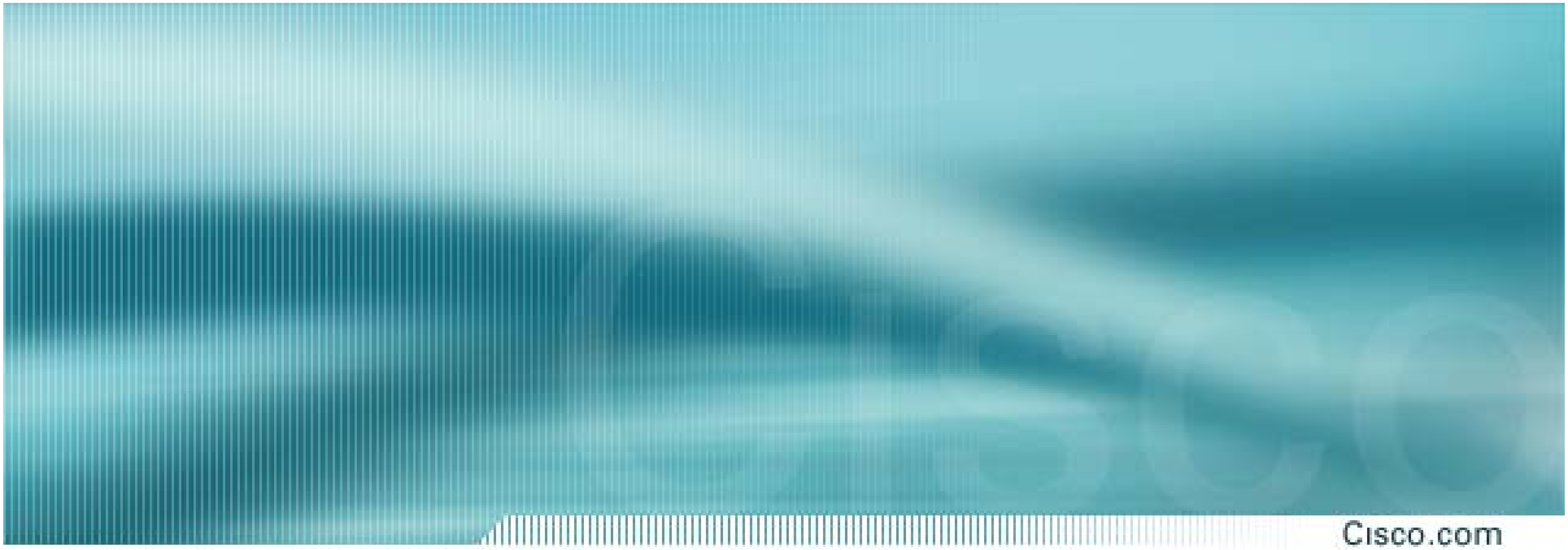
Catalyst—Multilayer Switching

DLSW over Ethernet

Catalyst

Catalyst

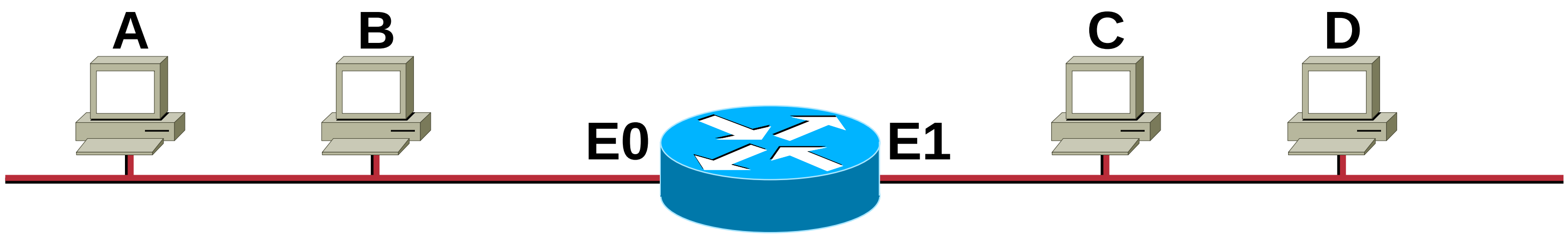
- Spanning Tree
- Cat3550
- VTP
- Layer2
- Layer3



Catalyst—Spanning Tree

Transparent Bridging Overview

- Transparent bridging is a means to connect networks together at the data-link layer



Bridge Table

Mac Addr	Interface
A	E0
B	E0
C	E1
D	E1

Spanning Tree Overview

- STP calls for the election of the root switch
- Bridges/switches transmit BPDU frames to communicate
- Bridge protocol data units are sent every two seconds by default
- STP ports have five states—blocking, listening, learning, forwarding, or disabled
- STP forces redundant data paths into a standby (blocked) state

BPDU—Bridge Protocol Data Unit

What's in a BPDU?

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

Spanning Tree Timers

- **Hello timer**

  Determines how often the switch broadcasts hello messages to other switches

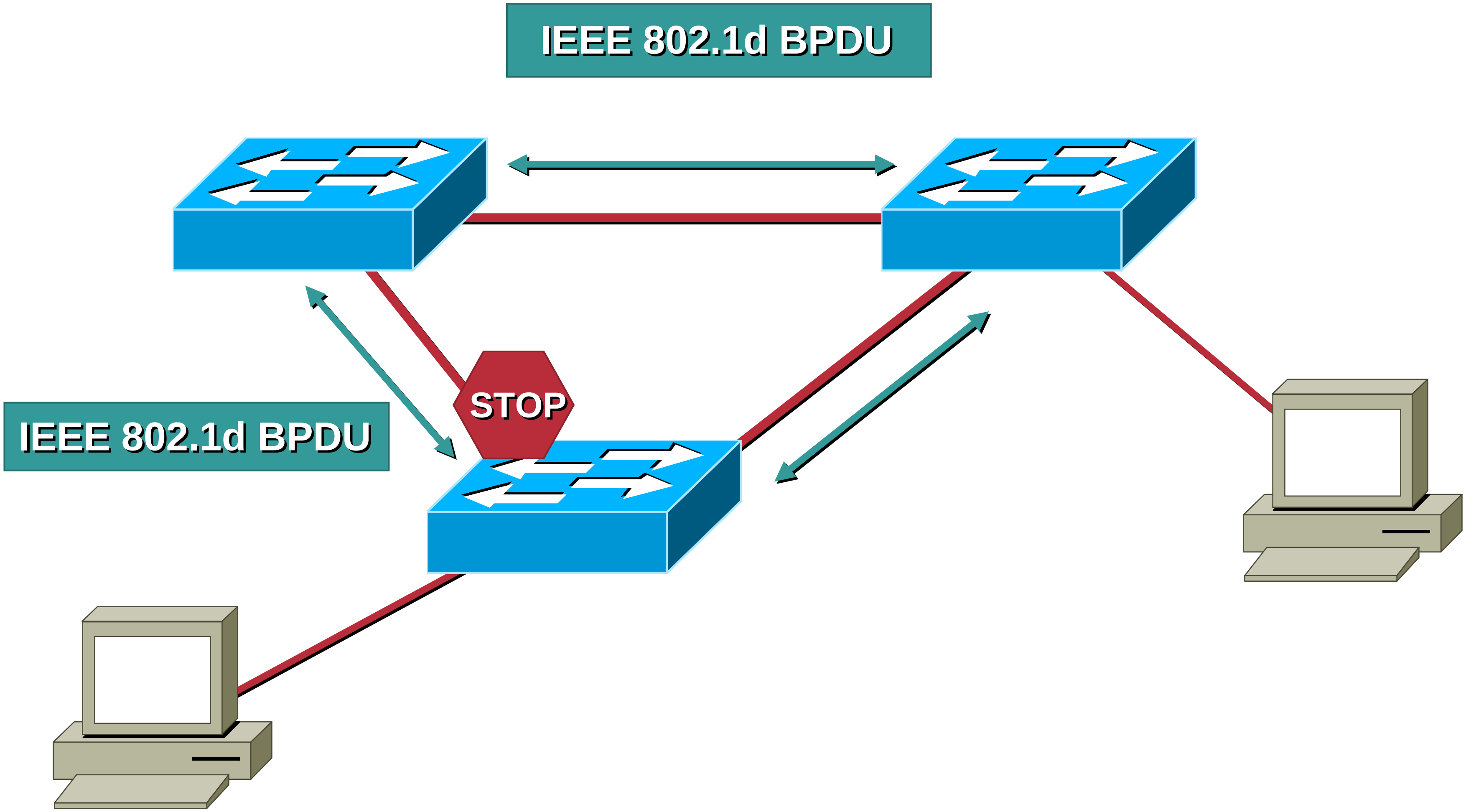
- **Forward-delay timer**

  Determines how long each of the listening and learning states last before the interface begins forwarding

- **Maximum-age timer**

  Determines the amount of time the switch stores protocol information received on an interface

Spanning Tree Protocol in Action



Spanning Tree Commands

Configuring the Root Switch—(CatOS *set spantree root)*

spanning-tree vlan [*vlan-id]* root [primary/secondary]

```
Switch(config)#spanning-tree vlan 100 root primary
 vlan 100 bridge priority set to 24576
 vlan 100 bridge max aging time unchanged at 20
 vlan 100 bridge hello time unchanged at 2
 vlan 100 bridge forward delay unchanged at 15
Switch(config)#
```

Bridge Priority Gets Set to 24567 Or 4096 Less than the Current Root Priority, Whichever Is Less

Verify STP (CatOS *show spantree*)

Show spanning-tree [vlan]—to view spanning tree information

```
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000a.41d6.7e00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000a.41d6.7e00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Port ID                   Designated             Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID          Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Fa0/24           128.20        19 FWD         0 32769 000a.41d6.7e00 128.20
Fa0/13           128.21        19 FWD         0 32769 000a.41d6.7e00 128.21
Fa0/14           128.22        19 FWD         0 32769 000a.41d6.7e00 128.22
Fa0/15           128.23        19 FWD         0 32769 000a.41d6.7e00 128.23
Fa0/16           128.24        19 FWD         0 32769 000a.41d6.7e00 128.24
```

Which VLAN

Designated Root Information

This Bridge Information

Port States and Cost

Spanning Tree Review

- Spanning tree is a link management protocol that provides path redundancy while preventing undesirable loops in the network
- Spanning tree operation is transparent to end stations
- Catalyst enterprise LAN switches use the Spanning Tree Protocol, IEEE 802.1D
- A single instance of STP runs on each configured VLAN
- Spanning tree defines a tree with a root switch and a loop-free path from the root to all switches in the extended layer 2 network

Spanning Tree

Switch Commands—STP

*forward-time	Set the Forward Delay for the Spanning Tree
*hello-time	Set the Hello Interval for the Spanning Tree
*max-age	Set the Max Age Interval for the Spanning Tree
***priority	Set the Bridge Priority for the Spanning Tree
***root	Configure Switch as Root
**backbonefast	Enable BackboneFast Feature
**etherchannel	Spanning Tree EtherChannel Specific Configuration
*extend	Spanning Tree 802.1t Extensions
***pathcost	Spanning Tree Pathcost Options
***portfast	Spanning Tree Portfast Options
**uplinkfast	Enable UplinkFast Feature

Importance: ***High **Medium *Low

Transparent Bridging

- Basic bridging example—the system has two Ethernets and one serial line; IP traffic is routed and everything else is bridged

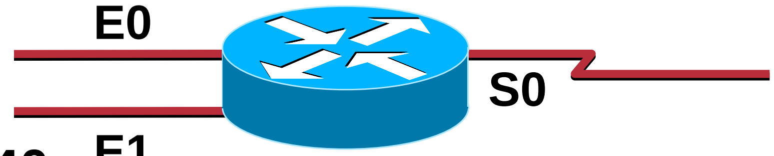
```
interface Ethernet 0
  ip address 192.31.7.26 255.255.255.240
  bridge-group 1
!
interface Ethernet 1
  ip address 192.31.7.65 255.255.255.240
  bridge-group 1
!
interface serial 0
  ip address 192.31.7.34 255.255.255.240
  bridge-group 1
!
bridge 1 protocol ieee
```

Bridging Is Enabled

Bridging Is Enabled

Bridging Is Enabled

Spanning Tree Is Enabled



Integrated Routing and Bridging

Integrated Routing and Bridging Allows Bridged and Routed Traffic of the Same Protocol to Be Interchanged

```
interface Ethernet 0
  bridge-group 1
!
interface Ethernet 1
  bridge-group 1
!
interface Ethernet 2
  bridge-group 1
!
interface Ethernet 3
  ip address 5.0.0.1 255.0.0.0
!
interface BVI 1
  ip address 3.0.0.1 255.0.0.0
!
bridge irb
bridge 1 protocol ieee
  bridge 1 route ip
```

Bridging Is Enabled

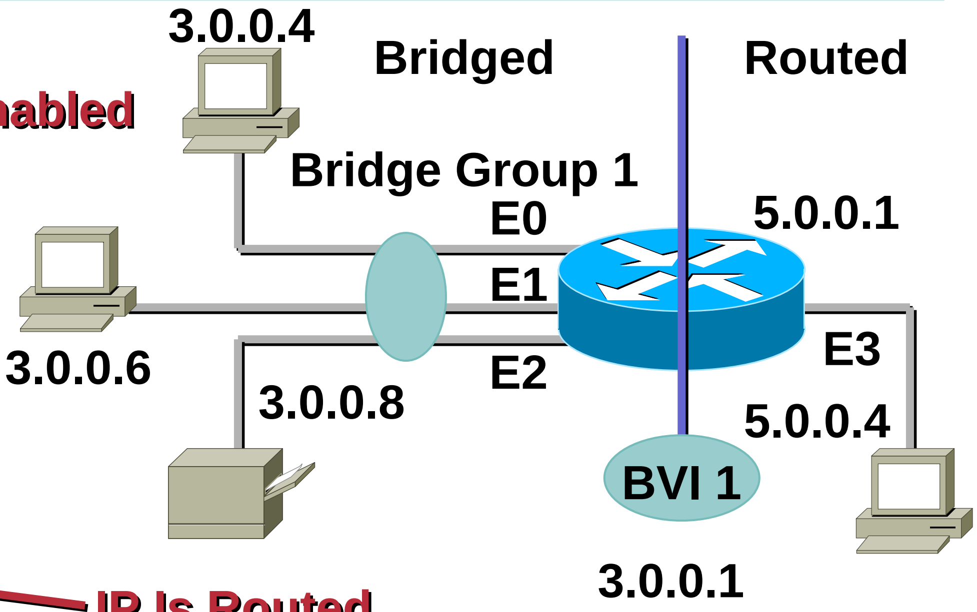
IP Is Routed

Bridge Virtual Interface Is Created

BVI IP Address Assigned

IRB Is Enabled

IP Is Bridged and Routed Over BVI



IP Is Routed and Bridged via Bridge Group 1

Catalyst 3550

- Each candidate rack will consist of 2 (two) Catalyst 3550 switches with the Enhanced Multilayer Image-EMI IOS Software

Terminology Review

- **Catalyst VTP**—VLAN Trunk Protocol

  VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis

- **Catalyst VTP Domain**—VLAN management domain

  One or more interconnected switches that share the same VTP domain name

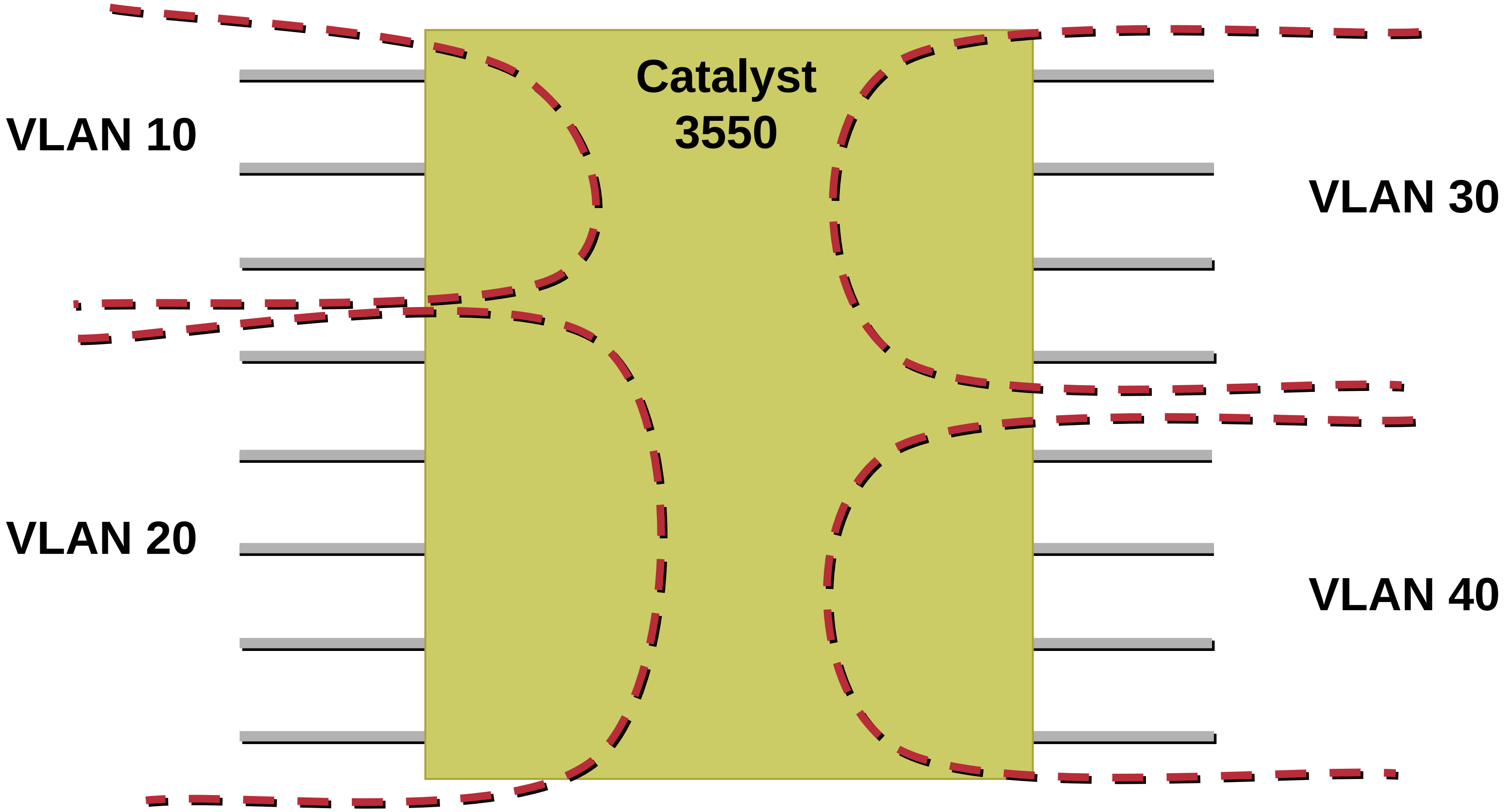
- **EMI**—Enhanced Multilayer Image

  Cisco IOS 12.1 EMI The layer2/3 IOS software for Catalyst 3550

- For more information check CCO at the following url:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/

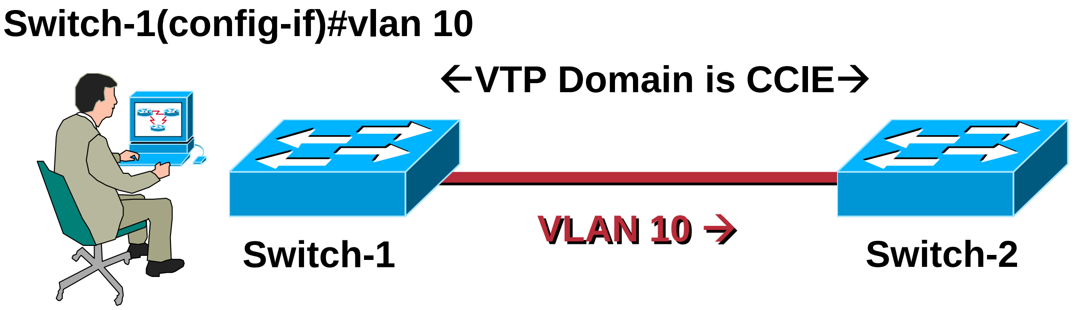
Switching Overview



Ports Are Assigned to Vlans
Ports Are in VLAN 1 by Default
Each VLAN Is a Separate Layer 2 Domain
Traffic Is Switched **Within** a VLAN, Not **between** VLANS
A Separate Instance of STP Is Run per VLAN

VTP—VLAN Trunk Protocol

- VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis
- Switches must be in the same VTP domain to share VLAN information



Verify VTP

```
Switch#show vtp status
VTP Version                          : 2
Configuration Revision               : 1
Maximum VLANs supported locally      : 1005
Number of existing VLANs             : 12
VTP Operating Mode                   : Server
VTP Domain Name                      : CCIE-LAB
VTP Pruning Mode                     : Disabled
VTP V2 Mode                          : Disabled
VTP Traps Generation                 : Disabled
Configuration last modified by 1.1.1.1 at 3-1-93 04:16:16
Local updater ID is 1.1.1.1 on interface Vl1
```

Switch Commands—VTP

***domain	Set the Name of the VTP Administrative Domain
*Interface	Preferred Source for the VTP IP Updater Address
***mode client	Set the Device to Client Mode
***mode server	Set the Device to Server Mode
***mode transparent	Set the Device to Transparent Mode
*file	IFS File System File where VTP Configuration Is Stored
**pruning	Set the Administrative Domain to Permit Pruning
*v2-mode	Set the Administrative Domain to v2 Mode
*password	Set the Password for the VTP Administrative Domain

Importance: ***High **Medium *Low

Catalyst 3550 and VLAN’s

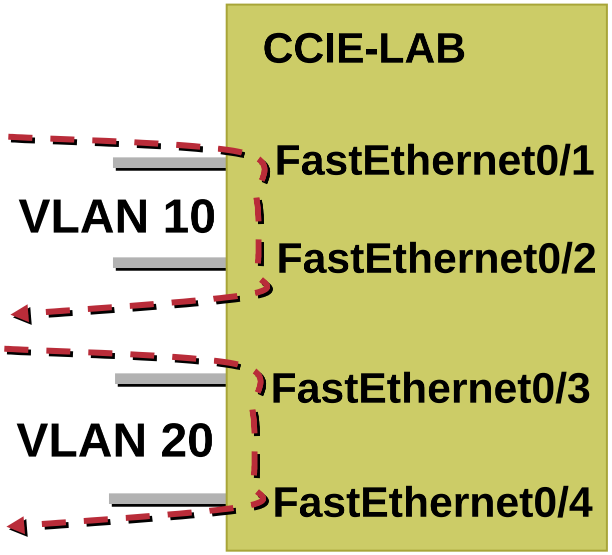
- The Catalyst 3550 switch supports 1005 VLANs in VTP client, server, and transparent modes
- VLANs are identified with a number from 1 to 4094
- VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs
- VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database
- The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094

VLAN Configuration Mode Options

- **Config-vlan mode**
- **Database mode**

Both methods produce the same results!

Config-vlan Mode—Commands

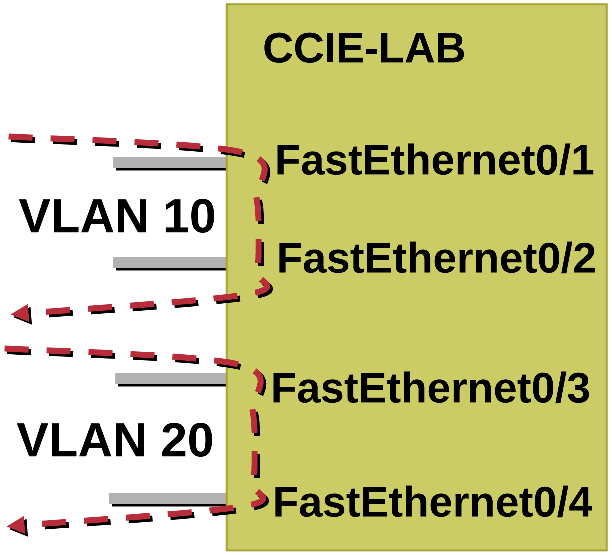


```
Switch#conf t
Switch(config)#vtp mode server
Switch(config)#vtp domain CCIE-LAB
Switch(config)#vlan 10
Switch(config)#vlan 20
Switch(config-vlan)#end
Switch#
```

VTP Domain of the Switch

Create VLAN's

Database Mode—Commands



CCIE-LAB

VLAN 10

FastEthernet0/1

FastEthernet0/2

VLAN 20

FastEthernet0/3

FastEthernet0/4

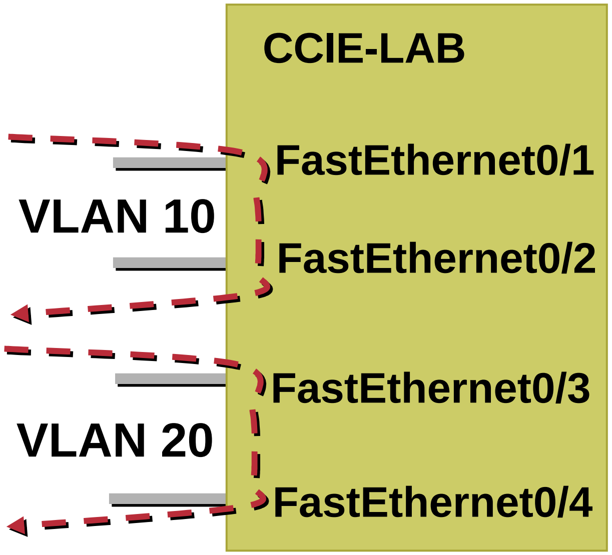
```
Switch#vlan database
Switch(vlan)#
Switch(vlan)#vtp server
Switch(vlan)#vtp domain CCIE-LAB
Switch(vlan)#vlan 10
Switch(vlan)#vlan 20
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#
```

VTP Domain of the Switch

Create VLAN’s

Changes Saved in Database

VLAN Port Assignments—Commands



```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
….
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

Interface Defined as Layer 2 Access Port

VLAN Assignment

Verify VLAN's

Switch#**show vlan brief**

```
VLAN Name                  Status      Ports
---- ---------------       ----------- -------------------------------
1    default               active      Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                       Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                       Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                       Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                       Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                       Gi0/1, Gi0/2
10   R2-R3                 active      Fa0/1
20   VLAN0020              active      Fa0/2
30   VLAN0030              active      Fa0/3, Fa0/10
36   VLAN_A                active
40   VLAN_BB2              active
62   VLAN_B                active
99   VLAN0099              active
187  VLAN0187              active
```

Verify Switchport

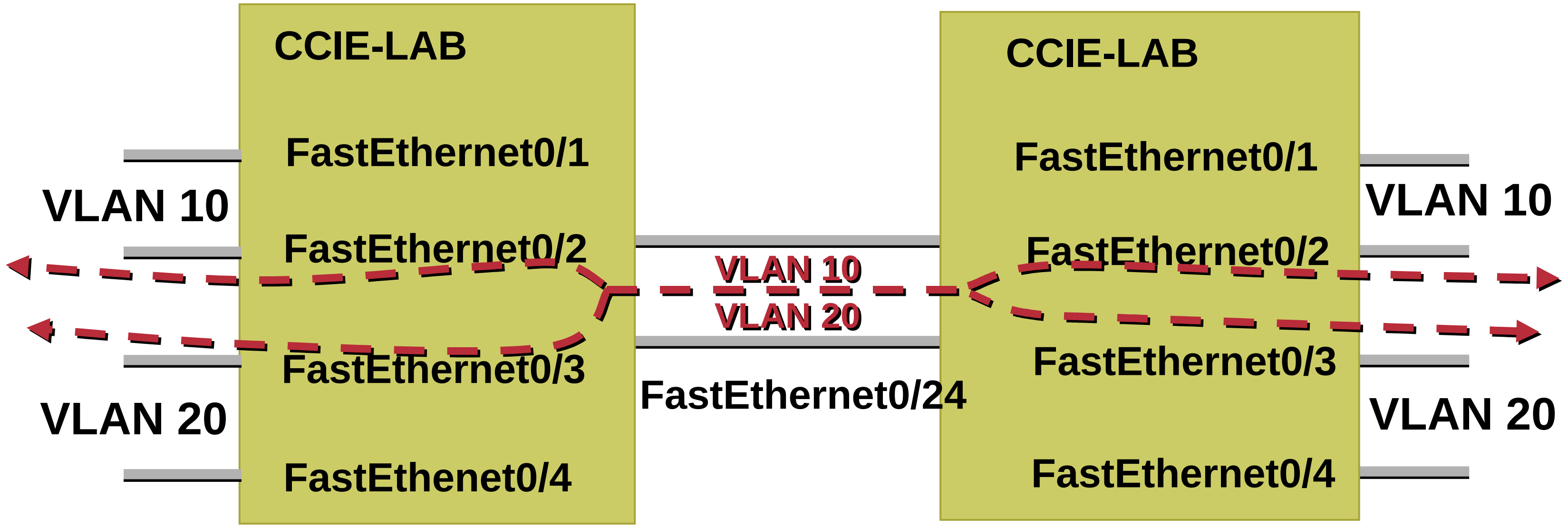
Cisco.com

```
Switch#show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (test)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Trunking

Carries the Traffic of Multiple Vlans over a Single Link

Configured on Fast Ethernet or Gigabit Ethernet Ports or Channels



```
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation isl
```

FastEthernet0/24 Set for Isl Trunking

Verify Trunk

```
Switch#show interfaces trunk

Port      Mode         Encapsulation        Status     Native vlan
Fa0/24     on                 isl            trunking     1

Port      Vlans allowed on trunk
Fa0/24     1-4094

Port      Vlans allowed and active in management domain
Fa0/24     1,10,20,30,36,40,62,99,187

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24     1,10,20,30,36,40,62,99,187
```

Troubleshooting Commands
show version

- **Show version—to view features and interfaces**

```
Switch#sh version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(9)EA1c, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 28-May-02 10:31 by antonino
Image text-base: 0x00003000, data-base: 0x00685778
ROM: Bootstrap program is C3550 boot loader
Switch uptime is 5 hours, 17 minutes
System returned to ROM by power-on
System image file is "flash:c3550-i5q3l2-mz.121-9.EA1c"
cisco WS-C3550-24 (PowerPC) processor (revision D0) with 65526K/8192K bytes of m
emory.
Processor board ID CHK0629V0CG
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
```

Cisco IOS Software

EMI Feature Set

Interfaces

Troubleshooting Commands

show int status

Show interface status [num]—to view port status

```
Switch#show interfaces status

Port    Name          Status      Vlan      Duplex  Speed Type
Fa0/1                 connected   10        a-half   a-10 10/100BaseTX
Fa0/2                 notconnect  20          auto   auto 10/100BaseTX
Fa0/3                 notconnect  30          auto   auto 10/100BaseTX
Fa0/4                 notconnect  1          auto   auto 10/100BaseTX
Fa0/5                 notconnect  1          auto   auto 10/100BaseTX
Fa0/6                 notconnect  1          auto   auto 10/100BaseTX
Fa0/7                 notconnect  1          auto   auto 10/100BaseTX
Fa0/8                 notconnect  1          auto   auto 10/100BaseTX
Fa0/9                 notconnect  1          auto   auto 10/100BaseTX
Fa0/10                notconnect  30          auto   auto 10/100BaseTX
Fa0/11                notconnect  1          auto   auto 10/100BaseTX
Fa0/12                notconnect  1          auto   auto 10/100BaseTX
Fa0/13                connected   1         a-full  a-100 10/100BaseTX
Fa0/14                connected   1         a-full  a-100 10/100BaseTX
Fa0/15                connected   1         a-full  a-100 10/100BaseTX
Fa0/16                connected   1         a-full  a-100 10/100BaseTX
Fa0/17                notconnect  1          auto   auto 10/100BaseTX
Fa0/18                notconnect  1          auto   auto 10/100BaseTX
Fa0/19                notconnect  1          auto   auto 10/100BaseTX
Fa0/20                notconnect  1          auto   auto 10/100BaseTX
Fa0/21                notconnect  1          auto   auto 10/100BaseTX
```

Troubleshooting Commands

show int stats

- **View traffic sent and received**

show interfaces stats

```
Switch#sh interfaces stats
Interface Vlan1 is disabled
FastEthernet0/1
       Switching path   Pkts In   Chars In   Pkts Out  Chars Out
          Processor        1        64          14542    2228830
        Route cache         0        0             0         0
            Total           1       64          14542    2228830
FastEthernet0/2
       Switching path   Pkts In   Chars In   Pkts Out  Chars Out
          Processor        0       0        0       0
        Route cache        0       0        0       0
            Total          0       0        0       0
```

Troubleshooting Commands

- **show cdp neighbor detail**—to show neighbor devices

```
Console (enable) sho cdp nei de
Device-ID: Router
Device Addresses:
  IP Address: 10.6.1.53
Holdtime: 152 sec
Capabilities: ROUTER
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C5RSM Software (C5RSM-AJSV-M), Version 11.2(14)P,  RELEASE SOFTWARE
  Copyright (c) 1986-1998 by cisco Systems, Inc.
Platform: cisco RSP2
Port-ID (Port on Device): Vlan1
Port (Our Port): 3/1
```

Type of Device

IP Address of Neighbor

Type of Device

Neighbor Cisco IOS Level

Type of Router

Which VLAN and Port The Neighbor Is on

```
Device-ID: 069046753
Device Addresses:
  IP Address: 10.10.10.1
Holdtime: 152 sec
Capabilities: TRANSPARENT_BRIDGE SR_BRIDGE SWITCH
Version:
  WS-C5500 Software, Version McpSW: 4.3(1a) NmpSW: 4.3(1a)
  Copyright (c) 1995-1998 by Cisco Systems
Platform: WS-C5500
Port-ID (Port on Device): 4/1
Port (Our Port): 4/1
```

IP Addr of Neighbor

Type of Device

Neighbor Cisco IOS Level

Type of Switch

Which VLAN and Port the Neighbor Is on

Troubleshooting Commands
show mac-address

- show mac-address-table [static /dynamic]

```
Switch#sh mac-address-table dynamic
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type      Ports
----    -----------       ----      -----
   1    000a.41c7.6800    DYNAMIC    Fa0/13
   1    000a.41c7.6801    DYNAMIC    Fa0/13
   1    000a.8a07.fe00    DYNAMIC    Fa0/14
   1    000a.8a07.fe01    DYNAMIC    Fa0/14
   1    000a.8a08.0880    DYNAMIC    Fa0/16
   1    000a.8a08.0881    DYNAMIC    Fa0/16
   1    000a.8a08.4c00    DYNAMIC    Fa0/15
   1    000a.8a08.4c01    DYNAMIC    Fa0/15
 100    000a.8a07.bf00    DYNAMIC    Fa0/23
 100    000a.8a07.bf13    DYNAMIC    Fa0/23
Total Mac Addresses for this criterion: 10
```

References

- Cisco LAN Switching, Kennedy Clark, Cisco Press
- Catalyst 3550 configuration guide CCO

  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550

Questions?

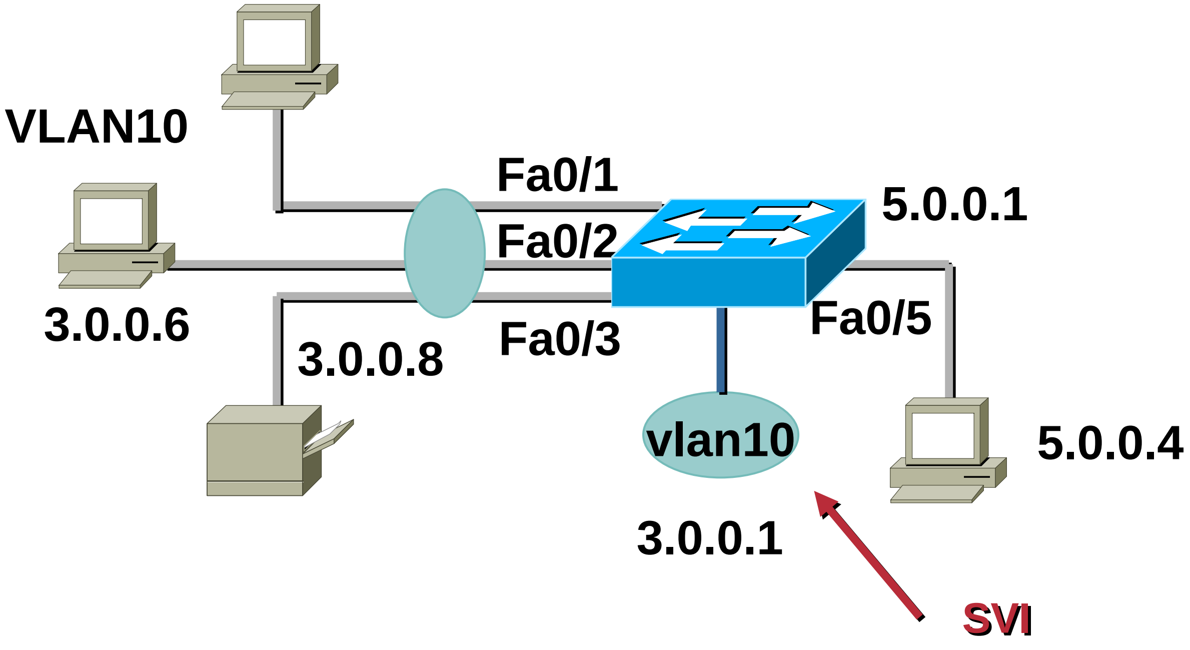
Catalyst—Layer 3

Layer 3 Interfaces

- **Switched Virtual Interface SVI**
- **Routed ports**

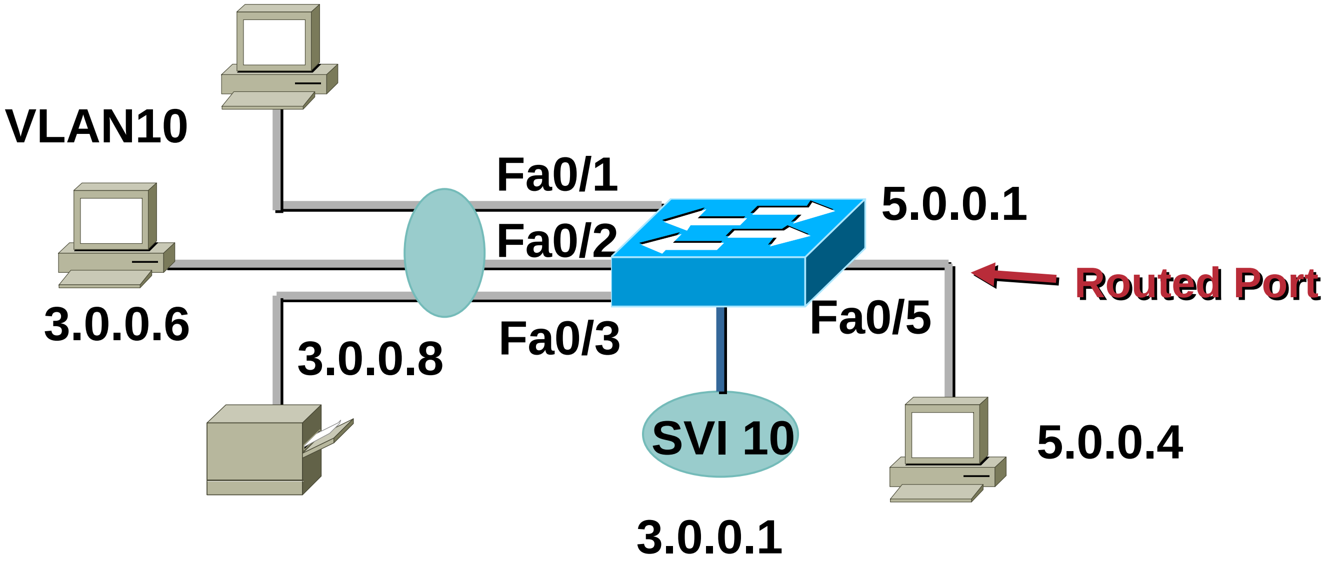
SVI—Switched Virtual Interface

- Software-based virtual interface
- Configure SVIs for any VLANs for which you want to route traffic
- SVI VLAN1 is created by default

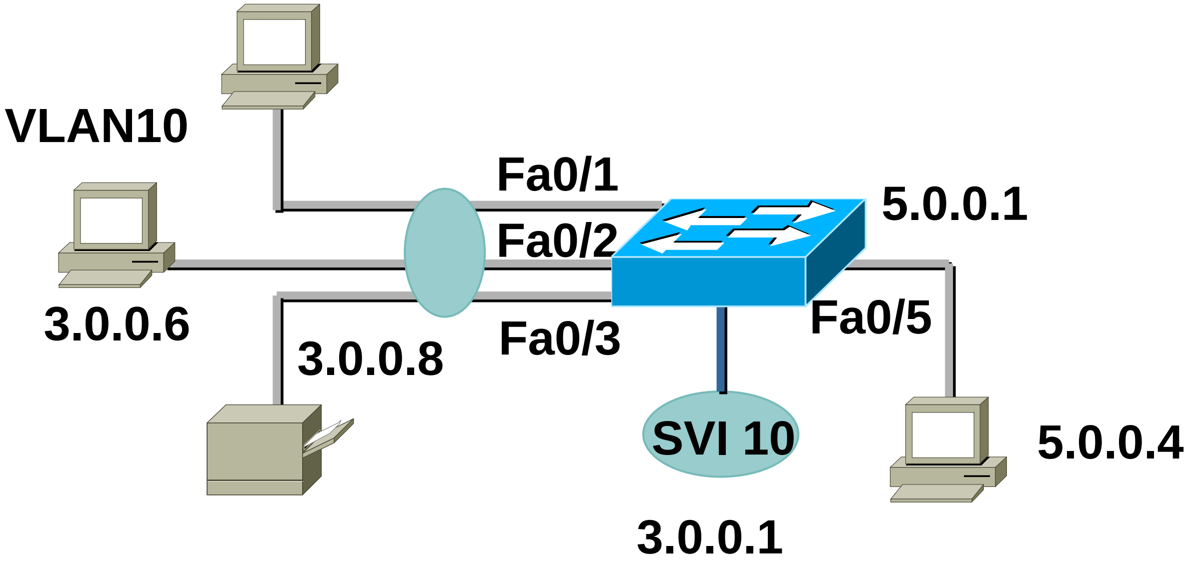


Routed Ports

- Acts like a port on a router
- Not associated with a particular VLAN
- Put the interface into Layer 3 mode with the *no switchport* interface configuration command



SVI—Routed Port Configuration



SVI

```
!
interface Vlan10
 ip address 3.0.0.1 255.0.0.0
end
```

Routed Port

```
!
interface FastEthernet0/5
 no switchport
 ip address 5.0.0.1 255.0.0.0
end
```

Catalyst Layer 3

- **Cat3550 with EMI behaves like a Cisco IOS router**
- **Practice RIP, EIGRP and OSPF using SVI and Routed interfaces**
- **IP Routing must be enabled first!**

Catalyst 3550—Cisco IOS Features

*Voice VLAN's	Carry IP *Voice* Traffic from an IP Phone
**SPAN	Switch Port Analyzer
**Security	General Security and ACL's
**QoS	Catalyst QoS
**EtherChannel	PaGP, Load Balancing, STP
*Fallback Bridging	Bridging Non-IP Protocols
*CDP	Cisco Discovery Protocol
*RMON	Remote Network Monitoring
***Unicast Routing	RIP, EIGRP,OSPF
***Multicast Routing	PIM SM, PIM DM, PIM SDM

802.1Q and Layer 2 Protocol Tunneling RESERVED FOR C/S EXAM

Importance: ***High **Medium *Low

References

- **Cisco LAN Switching, Kennedy Clark, Cisco Press**
- **Cisco Documentation**

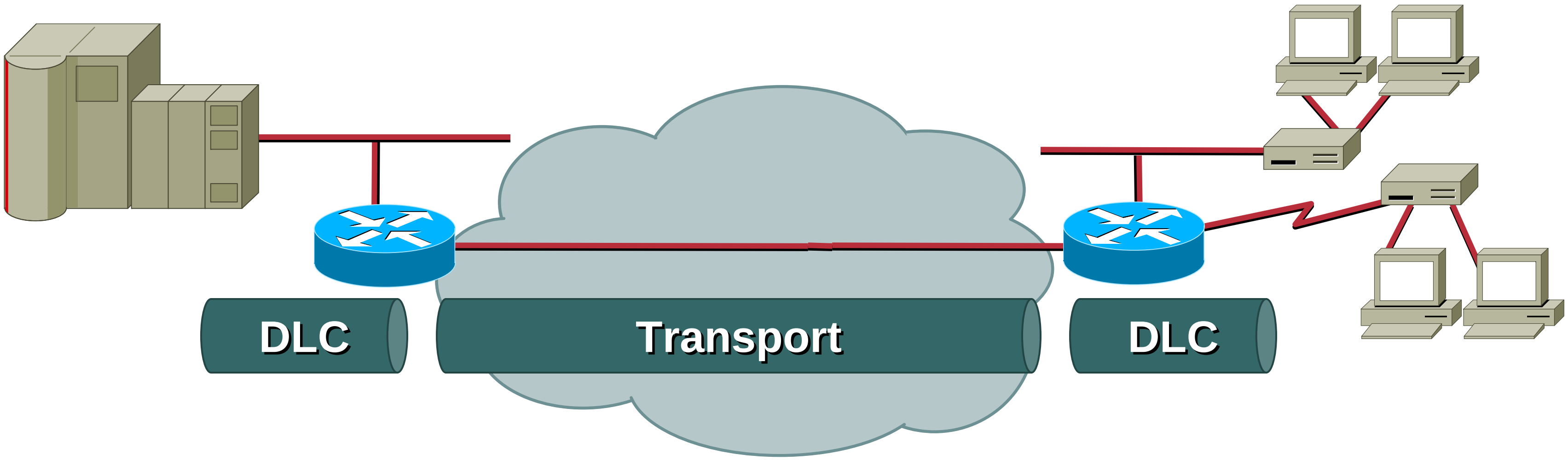
Questions?

DLSWoE

DLSW+

- **DLSW+**
- **DLSWoE Configuration**

What Is DLSw+

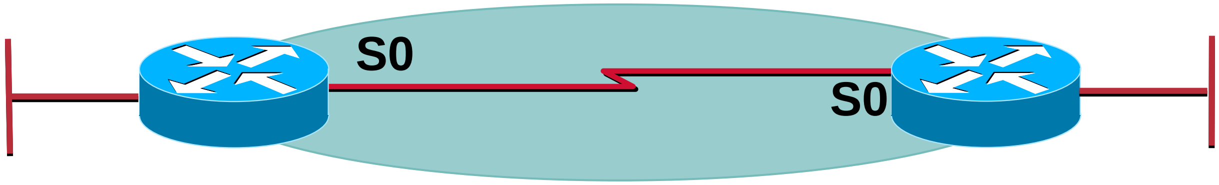


- Means to transport SNA and NetBIOS over multiprotocol backbone
- Fully compliant with DLSw standard
- Offers scalability, availability, and usability enhancements

5

DLSW+ over Ethernet

Example of DLSW—Simple Configuration



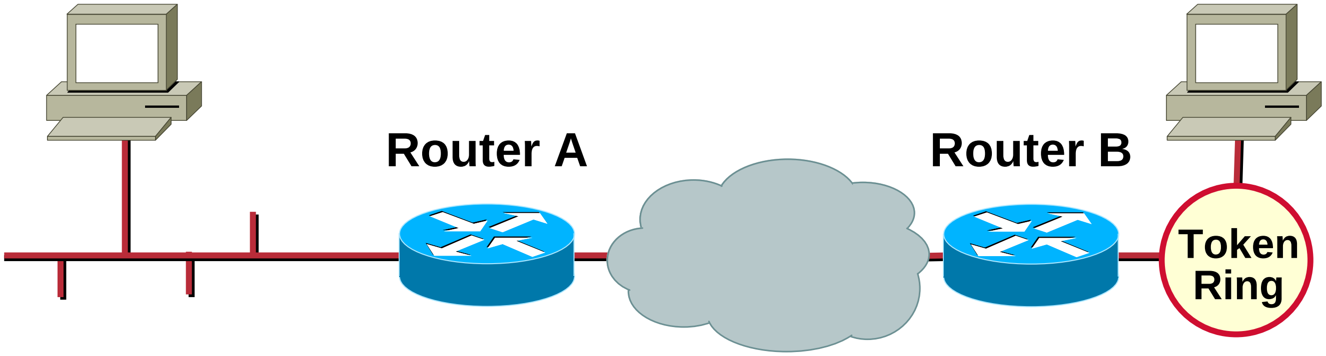
```
hostname RouterA
dlsw local-peer peer-id 10.1.1.1
dlsw remote-peer 0 tcp 10.1.1.2
dlsw bridge-group 1

interface Ethernet0
 ip address 5.1.1.1 255.255.255.0
 bridge-group 1

interface Serial0
 ip address 10.1.1.1 255.255.255.0

 bridge 1 protocol ieee
```

IP Address Must Match

```
hostname RouterB
dlsw local-peer peer-id 10.1.1.2
dlsw remote-peer 0 tcp 10.1.1.1
dlsw bridge-group 1

interface Ethernet0
 ip address 20.1.1.1 255.255.255.0
 bridge-group 1

interface Serial0
 ip address 10.1.1.2 255.255.255.0

 bridge 1 protocol ieee
```

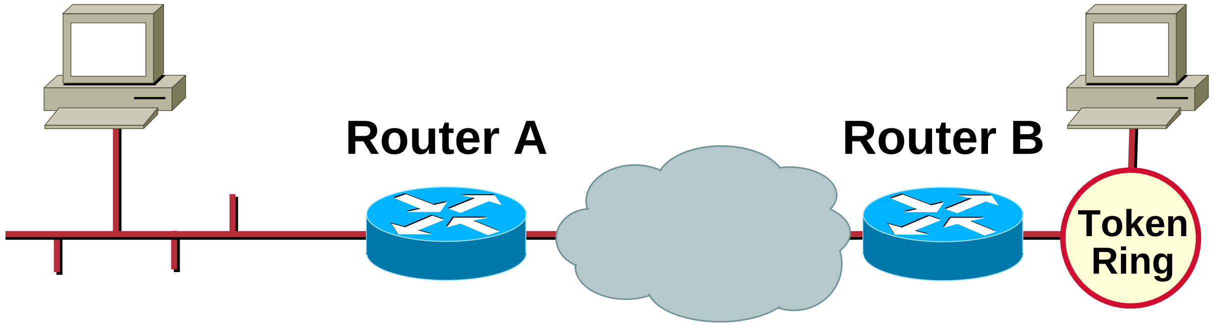
Troubleshooting DLSW

DLSW Show Commands



- show dlsw peers
- show spanning-tree
- show dlsw reachability

Show dlsw Peers



Remote Peer ID = 13.0.0.1

Local Peer ID = 14.0.0.1

Local Peer ID = 13.0.0.1

Remote Peer ID = 14.0.0.1

There Is One Circuit, i.e. One Session across Dlsw

```
Router A#sh dlsw peers
Peers:                state   pkts_rx  pkts_tx  type  drops ckts TCPq  uptime
 TCP 13.0.0.1         CONNECT   15998     8985  conf      0    1     0 2:46:46

Router B#sh dlsw peers
Peers:                state   pkts_rx  pkts_tx  type  drops ckts TCPq  uptime
 TCP 14.0.0.1         CONNECT    8996    16012  conf      0    1     0 2:50:41
```

If Not ‘CONNECT’ed, Troubleshoot Your IP Connectivity; Check Routes, IP Filters, etc.

Show spanning-tree

Verify That DLSW Is ‘Tied into’ the Transparent Bridging Domain

```
Router#sh spanning-tree
Port 5 (Ethernet0/0) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.5.
   Designated root has priority 32768, address 00e0.1e65.2d01
   Designated bridge has priority 32768, address 00e0.1e65.2d01
   Designated port id is 128.5, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 2
   BPDU: sent 95424, received 1185

Port 12 (DLSw Port0) of Bridge group 1 is forwarding
   Port path cost 10, Port priority 128, Port Identifier 128.12.
   Designated root has priority 32768, address 00e0.1e65.2d01
   Designated bridge has priority 32768, address 00e0.1e65.2d01
   Designated port id is 128.12, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 96469, received 0
```

← **bridge-group 1**

← **dlsw-bridge-group 1**

Show dlsw Reachability

DLSW Builds Its Reachability Cache as It Learns about End Stations

```
Router B#show dlsw reachability
DLSw MAC address reachability cache list
Mac Addr          status     Loc.     peer/port
0005.24b0.e21d    FOUND      REMOTE   13.0.0.1(2065)
```

End Station Mac Addrs

Status Is ‘FOUND’
Unless Circuit Is in Transition

End Station Is Either
LOCAL or REMOTE

Remote Peer if End
Station Is Remote

```
DLSw NetBIOS Name reachability cache list
NetBIOS Name      status     Loc.     peer/port
RED-DWARF         FOUND      REMOTE   13.0.0.1(2065)
```

End Station Netbios Names

Status Is ‘FOUND’
Unless Circuit Is in Transition

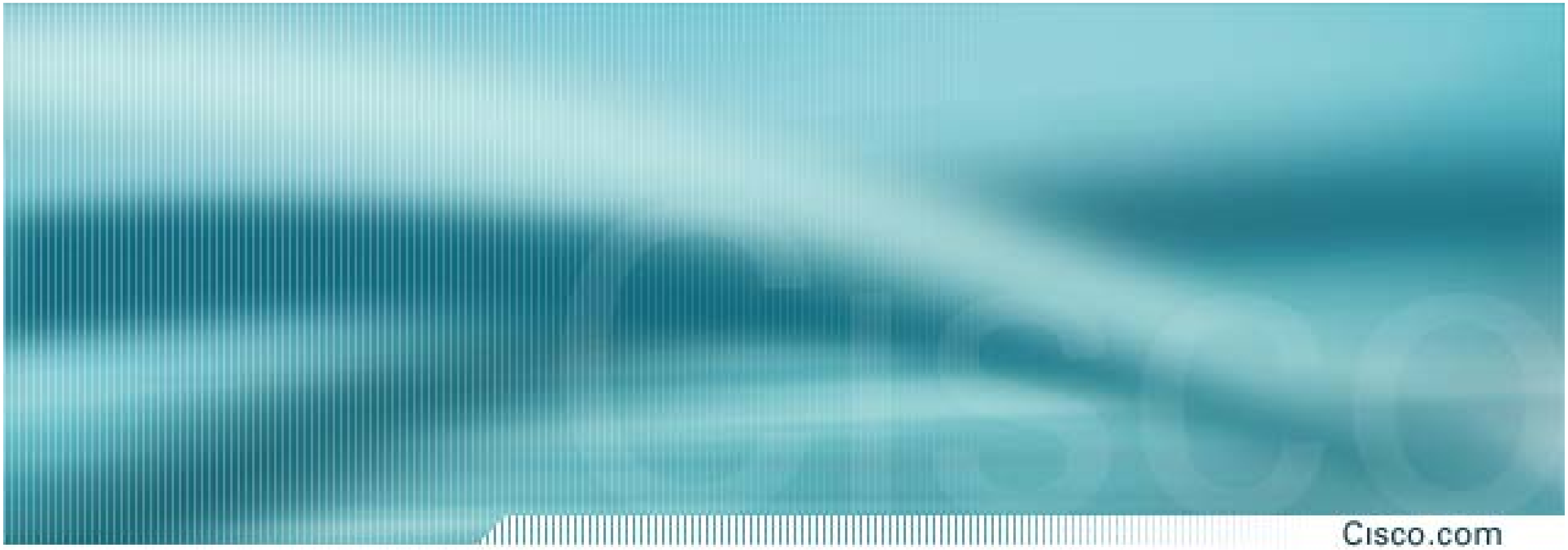
End Station Is Either
LOCAL or REMOTE

Remote Peer if End
Station is Remote

References

- Cisco Interactive Mentor, Multiprotocol Challenge, Cisco Press
- Cisco Documentation

Questions?



Session 3

QOS/IP Routing/RIP/EIGRP

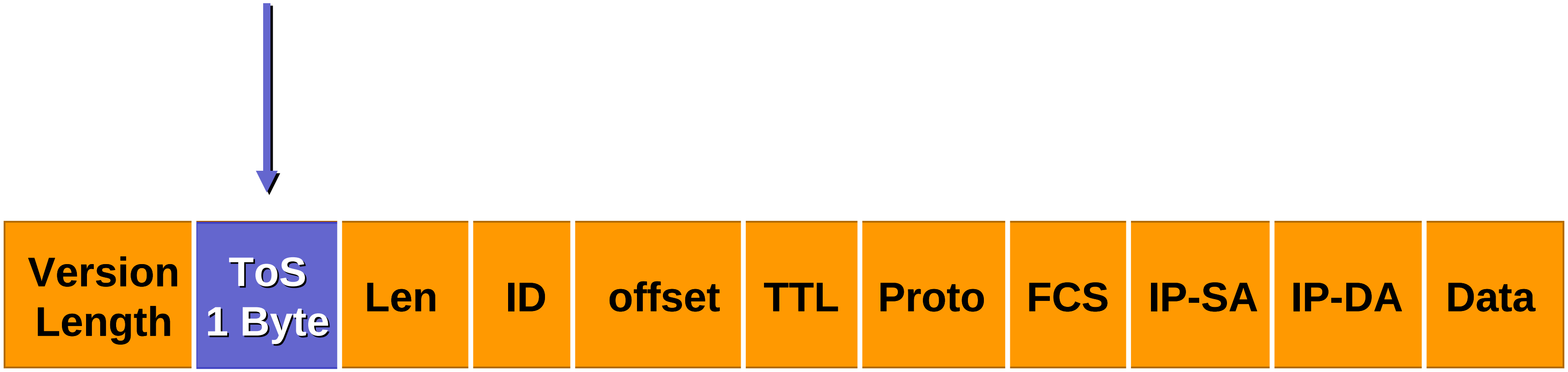
QoS Quality of Service

QoS—Quality of Service

- Traffic Classification
  - Policy-Based Routing
  - Committed Access Rate
  - Class-Based Weighted Fair Queuing
- Congestion Management
  - Weighted Fair Queuing
  - Class-Based Weighted Fair Queuing
  - Priority Queuing
  - Custom Queuing
- Congestion Avoidance
  - Weighted Random Early Detection

The Hook for Scalable IPv4 Packet-Marking and Classification

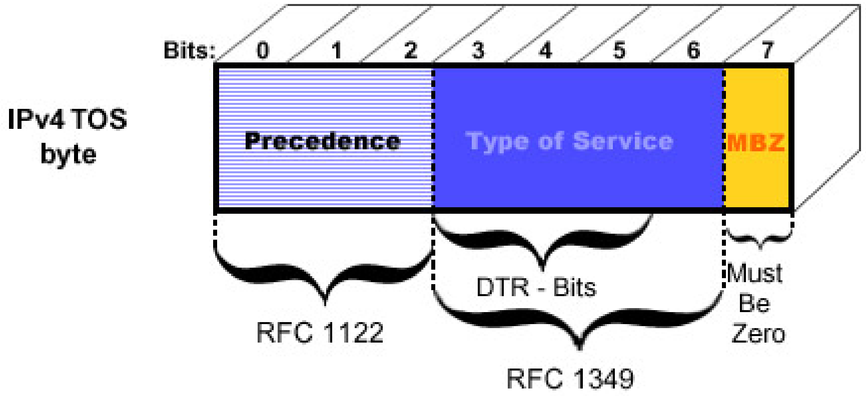
Packets Are Marked @ the Edge, for Purposes of Classification in the Core

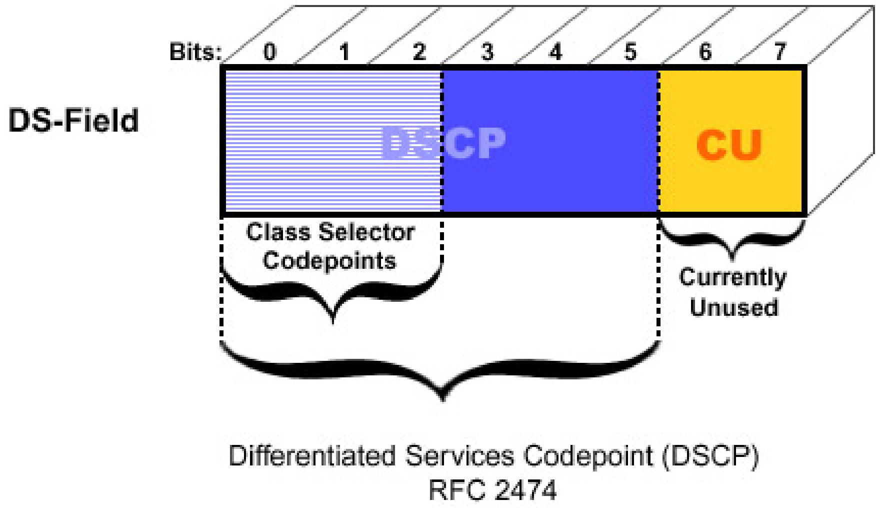


Version Length	ToS 1 Byte	Len	ID	offset	TTL	Proto	FCS	IP-SA	IP-DA	Data

The IPv4 Header and the Type of Service (ToS) Byte

IPv4 ToS vs. DS-Field (The ToS Byte Is Re-Defined)





Bits (0-2): IP- Precedence Defined

111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

Bits (3-6): The Type of Service Defined

0000 (all normal)
1000 (minimize delay)
0100 (maximize throughput)
0010 (maximize reliability)
0001 (minimize monetary cost)

DSCP

DS Field

DSCP

CU

DROP Precedence	*Class#1*	*Class #2*	*Class #3*	*Class #4*
Low Drop Precedence	AF11 (001010) 10	AF21 (010010) 18	AF31 011010) 26	AF41 (100010) 34
Medium Drop Prec	AF12 (001100) 12	AF22 (010100) 20	AF32 011100) 28	AF42 (100100) 36
High Drop Precedence	AF13 (001110) 14	AF23 (010110) 22	AF33 (011110) 30	AF43 (100110) 38

High Priority = EF = 101110 = 46   Best Effort = 000000 = 0

Policy-Based Routing

- Configured on the receiving interface
- Packets are routed based on a configured policy

Policy-Based Routing

- **Configuration steps:**

  Configure a route map to identify which packets will be policy routed

route-map example permit 10
 match length *min max*
 or
 match ip address *1 – 99 or 1300-1999* **(standard)**
 or
 match ip address *100 – 199 or 2000 – 2699* **(extended)**

Policy-Based Routing

Configuration Steps:

- **Configure a route map to classify and/or policy route the packets**

```
route-map example permit 10
 match length min max or match ip address
 set ip precedence 0-7 or name
```

critical	*Set critical precedence (5)*
flash	*Set flash precedence (3)*
flash-override	*Set flash override precedence (4)*
immediate	*Set immediate precedence (2)*
internet	*Set internetwork control precedence (6)*
network	*Set network control precedence (7)*
priority	*Set priority precedence (1)*
routine	*Set routine precedence (0)*

Policy-Based Routing

route-map example permit 10
 match length *min max* **or match ip address**
 set ip interface *interface name and number*

Forward Packet out the Indicated Interface if It Is up;
If It Is down then Use the IP Routing Table

set default interface *interface name and number*

Forward Using the IP Routing Table if a Route Exists;
If a Route Does Not Exist then Forward to the Indicated Interface

Policy-Based Routing

route-map example permit 10
 match length *min max* **or match ip address**
 set ip next-hop *IP address*

Forward Packet to the Indicated Next Hop if It Exists;
If Not, then Use the IP Routing Table

set ip default next-hop *IP address*

Forward Using the IP Routing Table if a Route Exists;
If a Route Does Not Exist then Forward to the Next Hop

Policy-Based Routing

Configuration Example:

```
access-list 1 permit ip 135.1.9.1
access-list 2 permit ip 135.1.9.2
!
interface ethernet 0/0
 ip policy route-map example
```

```
route-map example permit 10
 match ip address 1
 set ip precedence critical
 set ip default next-hop 135.1.20.3
!
route-map example permit 20
 match ip address 2
 set ip precedence routine
 set interface Serial0/0
```

Policy-Based Routing

- **Packets that are generated by the router are not normally policy-routed; to enable local PBR for such packets, indicate which route map the router should use by using the following command in global configuration mode:**

```
ip local policy route-map name
```

Policy-Based Routing

- **PBR can be fast-switched; prior to Cisco IOS Release 12.0, PBR could only be process-switched, which meant that on most platforms the switching rate was approximately 1000 to 10,000 packets per second; this speed was not fast enough for many applications; users that need PBR to occur at faster speeds can now implement PBR without slowing down the router; enable using the interface command:**

```
ip route-cache policy
```

The **set ip default next-hop** and **set default interface** commands are not supported.

Committed Access Rate

- Use on edge routers to classify and/or rate limit traffic
- Can be applied to all traffic or a subset of the traffic selected by an access list
- It is configured on the interface

Committed Access Rate

rate-limit {input|output} *bps normal-burst max-burst* **conform-action** *action* **exceed-action** *action*

rate-limit {input|output} access-group *index bps normal-burst max-burst* ***conform-action*** *action* ***exceed-action*** *action*

Committed Access Rate

bps	8000 – 2,000,000,000 bits per second
normal-burst	1000 – 512,000,000 bytes
max-burst	2000 – 1,024,000,000 bytes
index	IP access list number

action

continue	scan other rate limits
drop	drop packet
set-dscp-continue 0-63	set dscp, scan other rate limits
set-dscp-transmit 0-63	set dscp and send it
set-mpls-exp-continue 0-7	set exp, continue
set-mpls-exp-transmit 0-7	set exp and send it
set-prec-continue 0-7	rewrite precedence, continue
set-prec-transmit 0-7	rewrite precedence and send it
set-qos-continue 0-99	set qos-group, continue
set-qos-transmit 0-99	set qos-group and send it
transmit	transmit packet

Metering with Token Bucket

- Common rate measurement mechanism used by Policer and Shaper
- Components:

  Bc = Commited Burst

  Be = Excess Burst

  CIR = Committed Rate

  PIR = Peak Info. Rate

  CBS = Committed Burst Size

  PBS = Peak Burst Size

- Basic operation:

  Token bucket starts out full of Tokens

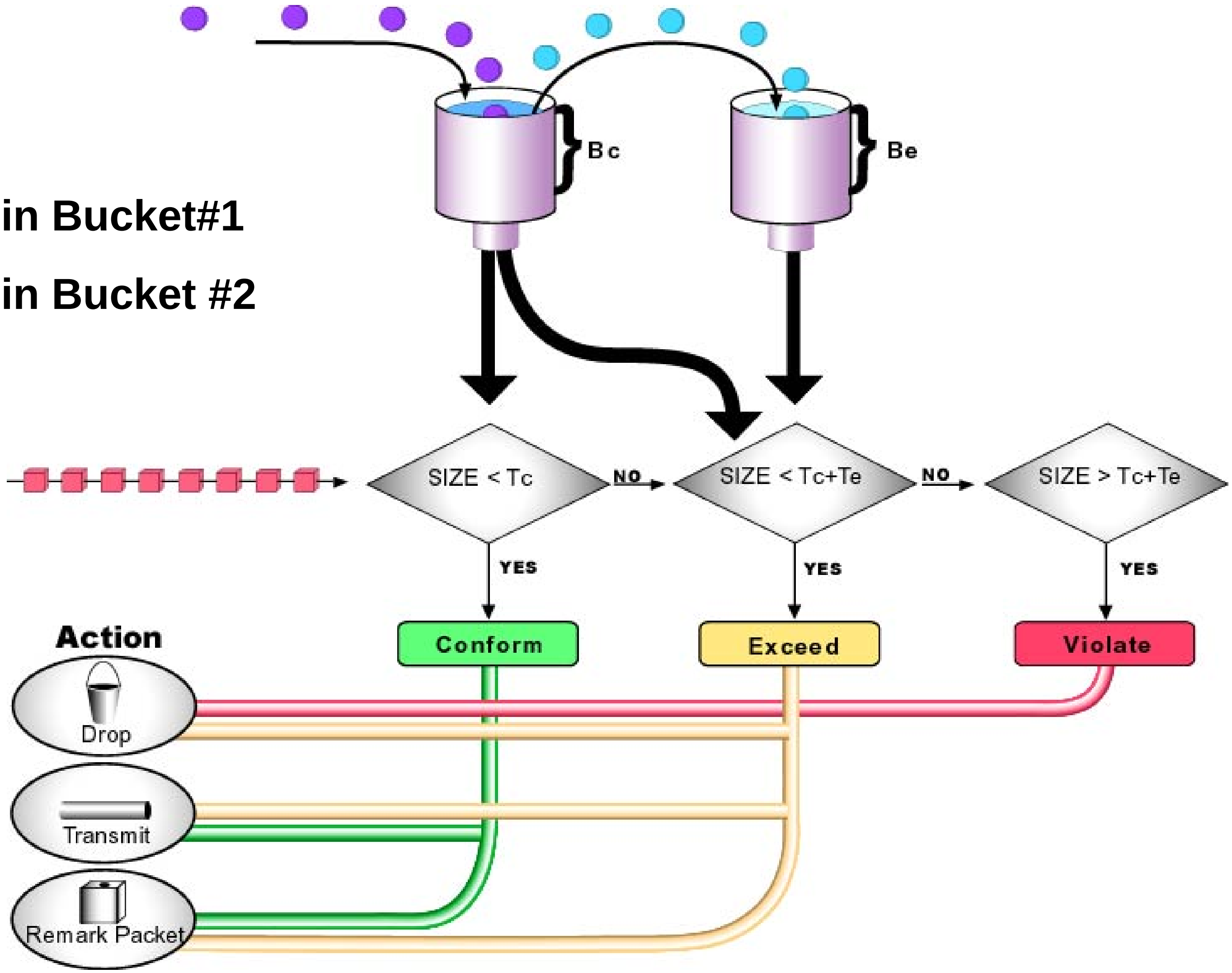
  #s of tokens based on CIR are added at delta T

  #s of tokens based on the size of the packet are removed from the token bucket upon forwarding that packet

RFC 2697: Single Rate Policer

Tc: Tokens in Bucket#1

Te: Tokens in Bucket #2



Conditions and Actions

- Conform Condition

  Bits-to-be-sent <= normal-burst (Bc)

- Exceed Condition

  normal-burst < bits-to-be-sent <= excess-burst (Be)

- Violate Condition

  bits-to-be-sent > excess burst (Be)

Actions: Drop/Transmit/Mark and Transmit

Committed Access Rate

Configuration Example:

- All World Wide Web traffic is sent; however, the IP precedence for web traffic that conforms to the first rate policy is set to 5; for nonconforming Web traffic, the IP precedence is set to 0 (best effort)
- File Transfer Protocol (FTP) traffic is sent with an IP precedence of 5 if it conforms to the second rate policy; if the FTP traffic exceeds the rate policy, it is dropped
- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 16,000 bytes and an Excess Burst size of 24,000 bytes; traffic that conforms is sent with an IP precedence of 5; traffic that does not conform is dropped

Committed Access Rate

Configuration Example:

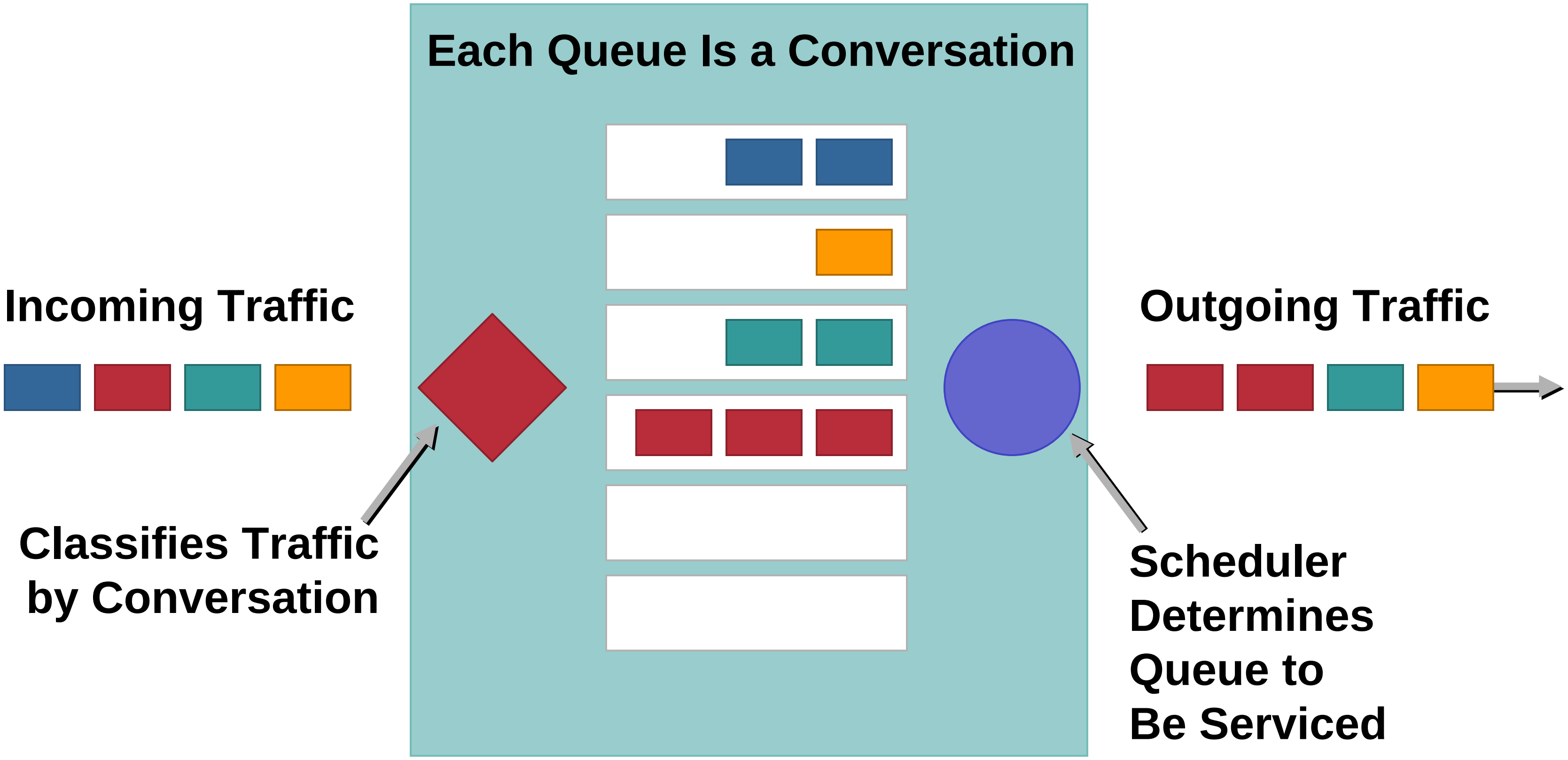
```
interface Hssi0/0/0
description 45Mbps to R2
rate-limit output access-group 101 20000000 24000 32000 conform-action set-prec-transmit 5 exceed-action set-prec-transmit 0
rate-limit output access-group 102 10000000 24000 32000 conform-action
set-prec-transmit 5 exceed-action drop
rate-limit output 8000000 16000 24000 conform-action set-prec-transmit 5
exceed-action drop
ip address 10.1.0.9 255.255.255.0
!
access-list 101 permit tcp any any eq www
access-list 102 permit tcp any any eq ftp
```

Weighted Fair Queuing

- Traffic is queued by flow
- A flow is a conversation between a source and a destination
- It is configured on the interface

Weighted Fair Queuing Chart

Cisco.com



Each Queue Is a Conversation

Incoming Traffic

Outgoing Traffic

Classifies Traffic
by Conversation

Scheduler
Determines
Queue to
Be Serviced

Weighted Fair Queuing Example

Discard Threshold of 100 Messages
500 Dynamic Queues
20 RSVP Queues

```
interface serial 0
  fair-queue 100 500 20
```

RSVP Queues
Default = 0

Discard Threshold
Default = 64

Dynamic Queues
Default = 256

Class-Based Weighted Fair Queuing (Modular QoS CLI)

- Traffic is queued by user defined classes
- A queue is reserved for each class
- Queue uses tail drop or WRED
- Unclassified traffic is flow-based

Class-Based Weighted Fair Queuing (Modular QoS CLI)

- **Step 1—Define the traffic classes**

Global Configuration

class-map *name*
class-map match-all *name*
class-map match-any *name*

name	name of the class map
match-all	**all clauses must match**
match-any	**any clause for a match**

Class-Based Weighted Fair Queuing (Modular QoS CLI)

Global Configuration

```
class-map match-any GOLD
 match
  access-group              Access group
  any                       Any packets
  class-map                 Class map
  cos                       IEEE 802.1Q/ISL class of service/user priority values
  destination-address       Destination address (MAC)
  input-interface           Select an input interface to match
  ip                        IP specific values
  mpls                      Multi Protocol Label Switching specific values
  not                       Negate this match result
  protocol                  Protocol
  qos-group                 Qos-group
  source-address            Source address (MAC)
```

Class-Based Weighted Fair Queuing (Modular QoS CLI)

Global Configuration

```
class-map match-any GOLD
 match protocol sqlnet
 match protocol ipsec
 match access-group 100
 match ip precedence 4 5

class-map match-all SILVER
 match access-group 101
 match access-group 102

class-map BRONZE
 match access-group 103
```

Class-Based Weighted Fair Queuing (Modular QoS CLI)

- **Step 2—Define the policy**

Global Configuration

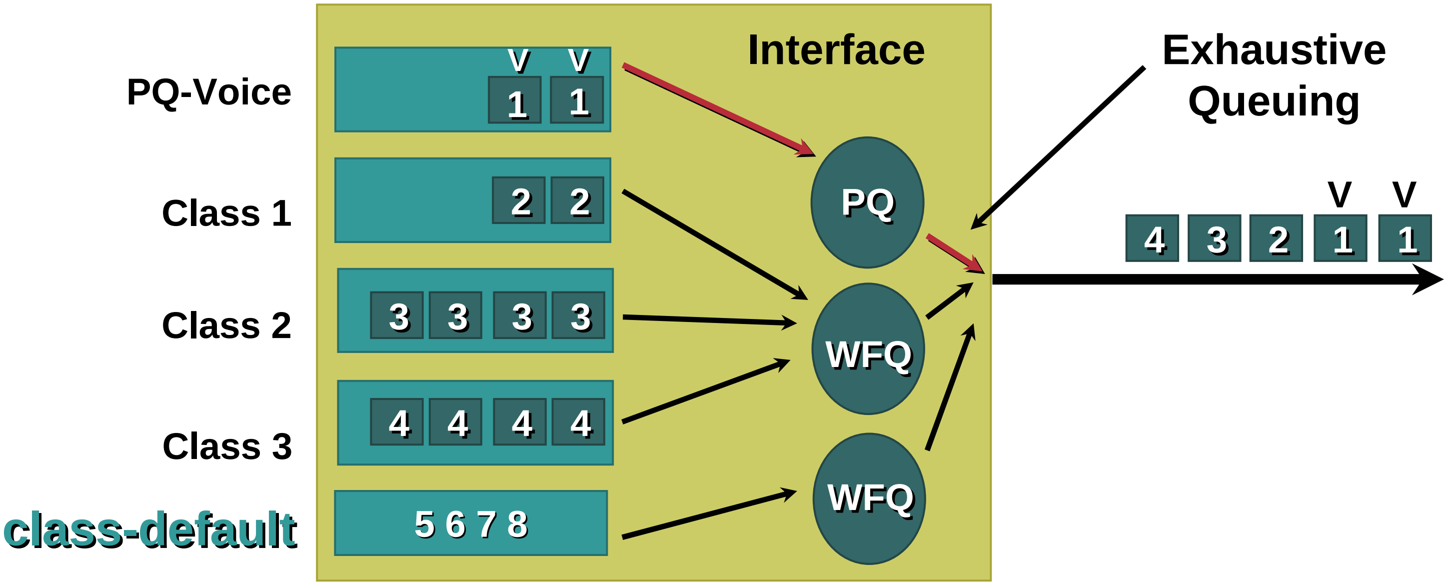
policy-map *name*	
class *class-map-name*	
bandwidth	kilobits/sec or percentage
queue-limit	(1 – 512 packets - for tail drop)
random-detect	(WRED)
shape	token bucket parameters
police	(CAR)
priority	Low Latency Queuing

Class-Based Weighted Fair Queuing (Modular QoS CLI)

- **Step 3—Apply the policy**

```
policy-map SERVICES
 class GOLD
  bandwidth 6000
 class SILVER
  bandwidth 3000
 class BRONZE
  bandwidth 700
 class class-default
   bandwidth 200

interface Ethernet 1/1
 service-policy output policy1
```

Low Latency Queuing



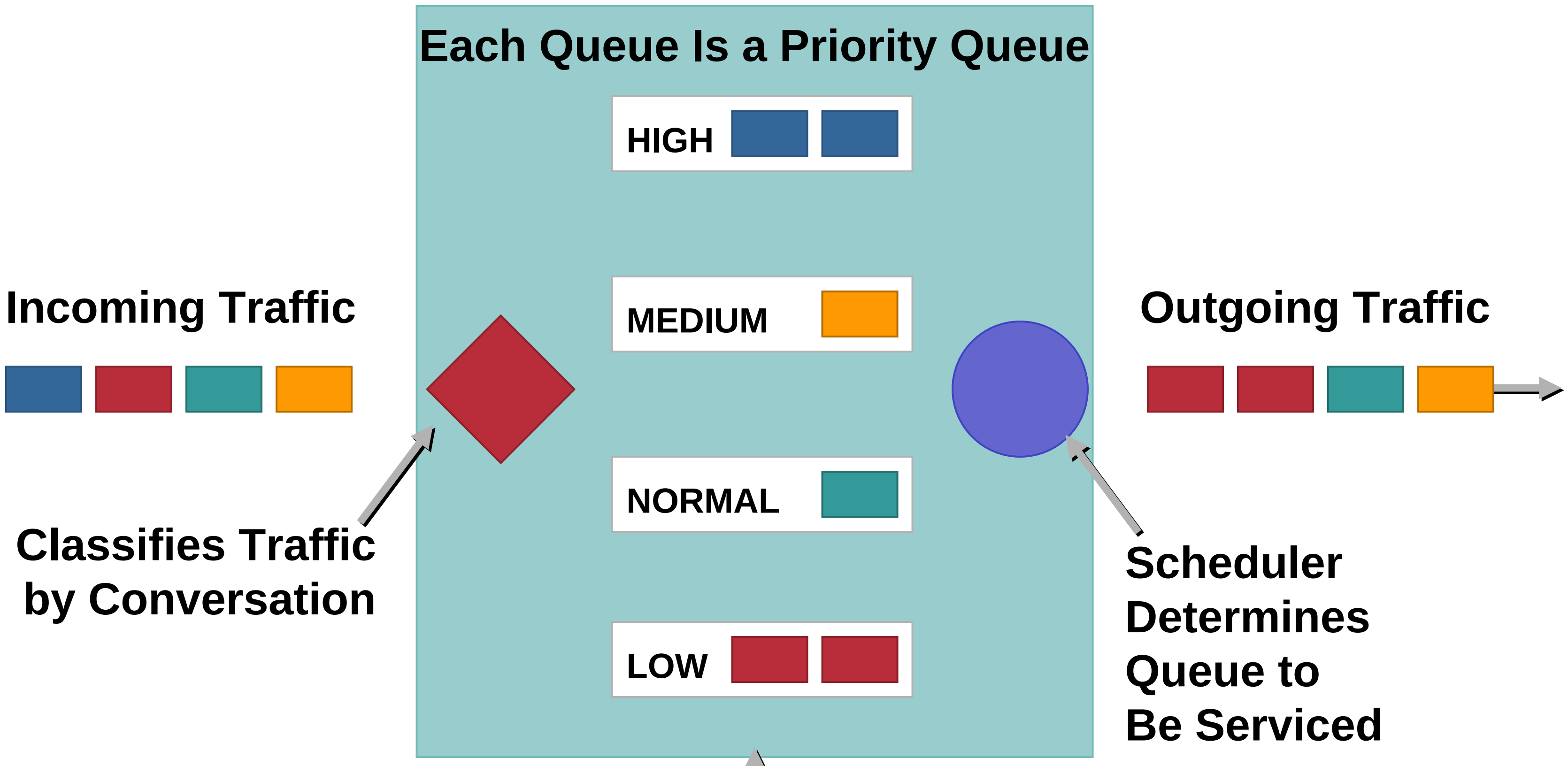
```
policy-map Multiservice
  class VoIP
    priority 240 (kilobits/sec)
```

Priority Queuing

- Traffic is queued by protocol and optionally port number
- Traffic is put into high, medium, normal, and low priority queues
- Traffic in higher priority queues will be serviced first
  - This may result in lower queues not getting serviced
- Queue depths can be configured
  - Default queue depths for high, medium, normal, and low are 20, 40, 60, and 80

Priority Queuing Chart

Cisco.com



Each Queue Is a Priority Queue

Incoming Traffic

Outgoing Traffic

HIGH

MEDIUM

NORMAL

LOW

Classifies Traffic by Conversation

Scheduler Determines Queue to Be Serviced

Queue Length Determined by Queue-Limit

Priority Queuing Example

SNA Traffic Is High Priority
WWW IP Traffic Is Low Priority
All Other IP Traffic Is Medium Priority
Set the Queue Depth for SNA Traffic to Be 50 Messages

```
interface serial 0
priority-group 1

priority-list 1 protocol sna high
priority-list 1 protocol ip low tcp 80
priority-list 1 protocol ip medium
priority-list 1 queue-limit 50 40 60 80
```

Apply Queues to Interface

SNA Is High Priority

WWW Is Low Priority

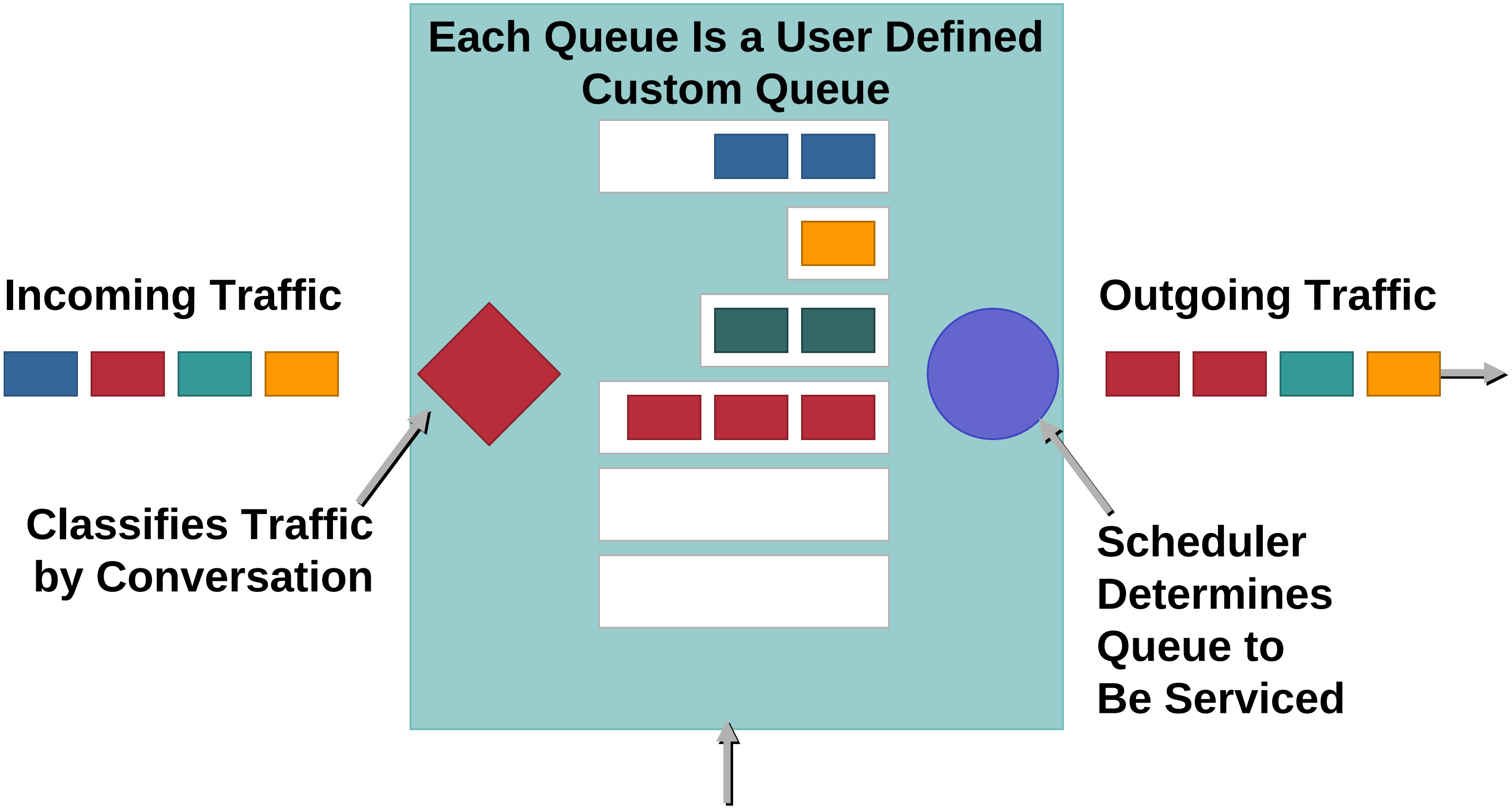
Other IP Traffic Is Medium Priority

High Priority Queue, SNA, Has a Queue Limit of 50

Custom Queuing

- Traffic is queued by protocol and optionally port number
- Traffic is put into user defined queues
- Traffic in each queue is serviced based on byte counts and queue depths
    - Once a queue's byte count limit is exceeded, the next queue is serviced
- Queue byte count limit and depths can be configured
    - Default queue byte count limit is 1500 bytes

Custom Queuing Chart



Each Queue Is a User Defined Custom Queue

Incoming Traffic

Outgoing Traffic

Classifies Traffic by Conversation

Scheduler Determines Queue to Be Serviced

Queue Length Determined by Queue-Limit

Custom Queuing Example

SNA Traffic Gets Triple the Bandwidth of All Other Traffic
IP Gets a Maximum of 3500 Bytes Serviced
IPX Gets a Maximum of 1500 Bytes Serviced

```
interface serial 0
custom-queue-list 1

queue-list 1 protocol sna 1
queue-list 1 protocol ip 2
queue-list 1 protocol ipx 3

queue-list 1 queue 1 byte-count 15000
queue-list 1 queue 2 byte-count 3500
queue-list 1 queue 3 byte-count 1500
```

Apply Queues to Interface

SNA, IP, and IPX Queues Are Defined in Queue-list 1

Queue 1, SNA, Is Set to 3 * (1500 + 3500) = 15000

Queue 2, IPX, Is Set to 3500 Bytes

Not Needed because 1500 Bytes Is the Default

Weighted Random Early Detection (WRED)

- Randomly drops packets prior to periods of high congestion
- Can use IP precedence to provide for preferential traffic handling of higher priority packets
- Attempts to anticipate and avoid congestion rather than control congestion once it occurs
- Uses a configurable exponential weighting constant

Weighted Random Early Detection (WRED)

```
interface Serial 0/1
 random-detect
```

Once random-detect is enabled then more configuration options appear

```
random-detect ?
 dscp                          parameters for each dscp value
 dscp-based                   Enable dscp based WRED on an interface
 exponential-weighting-constant  weight for mean queue depth calculation
 flow                         enable flow based WRED
 prec-based                   Enable prec based WRED on an interface
 precedence                   parameters for each precedence value
 <cr>
```

References

- **IP Quality of Service, Srinivas Vegesna Cisco Press**
- **Cisco Documentation**

Questions?

IP Routing Concepts

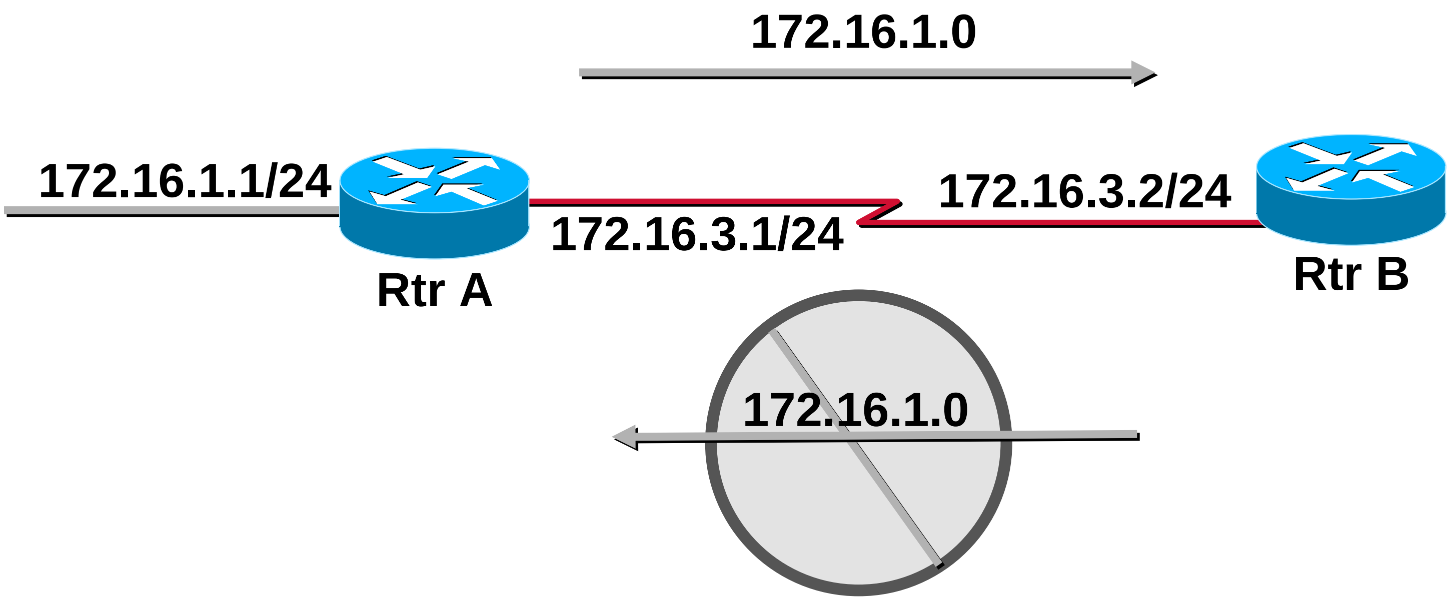
- Split Horizon
- Administrative Distance
- RIP/EIGRP Command Guide

IP Routing Concepts

Cisco.com

Split Horizon

- **Do not send a routing update out the interface on which it was learned**



IP Routing Concepts

Split Horizon

- Serial Interfaces

  Frame Relay not enabled—
  Split Horizon is enabled

  Frame Relay enabled, no sub-interface—
  Split Horizon is disabled

  Frame Relay enabled, sub-interfaces—
  Split Horizon is enabled

IP Routing Concepts

Administrative Distance

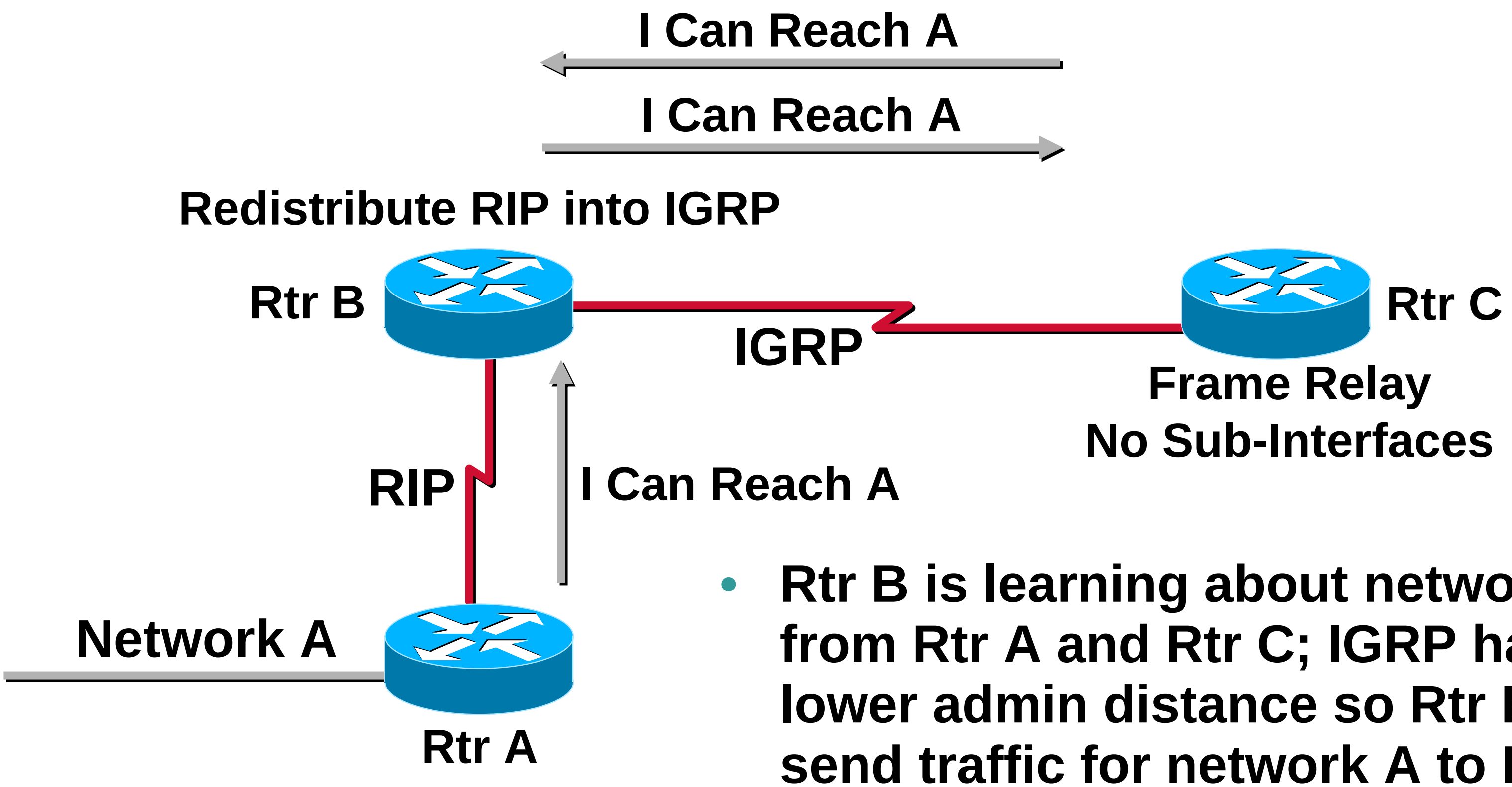
Connected	0
Static	1
EBGP	20
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
IBGP	200

- **A router with more than 1 IP routing protocol enabled will use the administrative distance to select a route if the route is learned from more than 1 protocol; a lower admin distance is preferred**

IP Routing Concepts

Cisco.com

Admin Distance and Split Horizon



- Rtr B is learning about network A from Rtr A and Rtr C; IGRP has a lower admin distance so Rtr B will send traffic for network A to Rtr C; Rtr C will send it back to Rtr B

Router Commands—RIP

*auto-summary	Enable Automatic Network Number Summarization
default	Set a Command to Its Defaults
**default-information	Control Distribution of Default Information
**default-metric	Set Metric of Redistributed Routes
**distance	Define an Administrative Distance
***distribute-list	Filter Networks in Routing Updates
exit	Exit From Routing Protocol Configuration Mode
*flash-update-threshold	Specify Flash Update Threshold in Second
help	Description of the Interactive Help System
*input-queue	Specify Input Queue Depth
*maximum-paths	Forward Packets over Multiple Paths

Importance: ***High **Medium *Low

Router Commands—RIP

**neighbor	Specify a Neighbor Router
**network	Enable Routing on an IP Network
no	Negate a Command or Set Its Defaults
*offset-list	Add or Subtract Offset from IGRP or RIP Metrics
output-delay	Interpacket Delay for RIP Updates
*passive-interface	Suppress Routing Updates on an Interface
***redistribute	Redistribute Information from Another Routing Protocol
*timers	Adjust Routing Timers
*traffic-share	Algorithm for Computing Traffic Share for Alternate Routes
*validate-update-source	Perform Sanity Checks against Source Address of Routing Updates
**version	Set Routing Protocol Version

Importance: ***High **Medium *Low

RIP/EIGRP

Router Commands—RIP

Rtr(config-if)#ip rip ?	
**Authentication	Authentication Control
**receive	Advertisement Reception
**send	Advertisement Transmission

Importance: ***High **Medium **Low

Router Commands—EIGRP

Router Configuration Commands:

*auto-summary	Enable Automatic Network Number Summarization
default	Set a Command to Its Defaults
**default-information	Control Distribution of Default Information
**default-metric	Set Metric of Redistributed Routes
**distance	Define an Administrative Distance
***distribute-list	Filter Networks in Routing Updates
*eigrp	EIGRP Specific Commands
exit	Exit From Routing Protocol Configuration Mode
help	Description of the Interactive Help System
*maximum-paths	Forward Packets over Multiple Paths

Importance: ***High **Medium *Low

Router Commands—EIGRP

Router Configuration Commands:

metric	Modify IGRP Routing Metrics and Parameters
**neighbor	Specify a Neighbor Router
**network	Enable Routing on an IP Network
no	Negate a Command or Set Its Defaults
*offset-list	Add or Subtract Offset from IGRP or RIP Metrics
*passive-interface	Suppress Routing Updates on an Interface
***redistribute	Redistribute Information from Another Routing Protocol
*timers	Adjust Routing Timers
*traffic-share	Algorithm for Computing Traffic Share for Alternate Routes
*variance	Control Load Balancing Variance

Importance: ***High **Medium *Low

RIP/EIGRP

Cisco.com

Router Commands—EIGRP

```
Rtr(config-if)#ip hello-interval eigrp 1 ?
  <1-65535>  Seconds Between Hello Transmissions
```

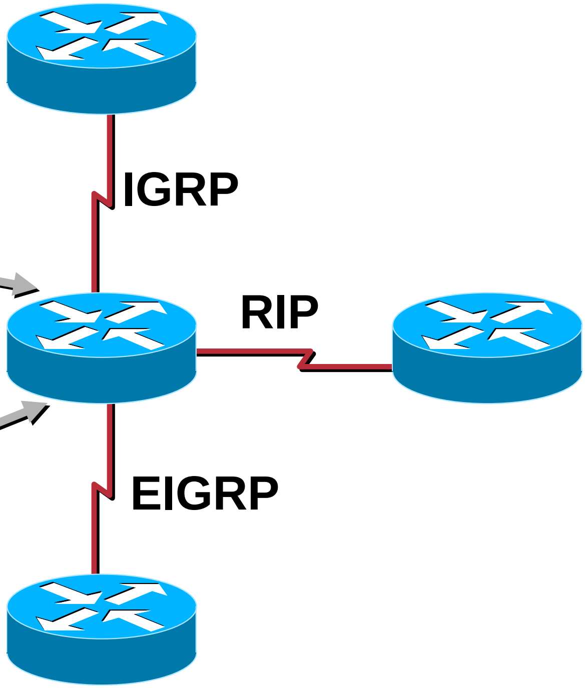
```
Rtr(config-if)#ip hold-time eigrp 1 ?
  <1-65535>  Seconds Before Neighbor is Considered Down
```

```
Rtr(config-if)#ip split-horizon eigrp ?
  <1-65535>  Autonomous System Number
```

RIP/EIGRP

Cisco.com

Route Redistribution



Redistribute igrp and eigrp into RIP; Assign All Routes a Metric (hop count) of 2

```
router rip
 redistribute igrp 1
 redistribute eigrp 3
 default-metric 2
```

Redistribute igrp and eigrp into RIP. Assign igrp routes a metric (hop count) of 1 and eigrp routes a metric of 2

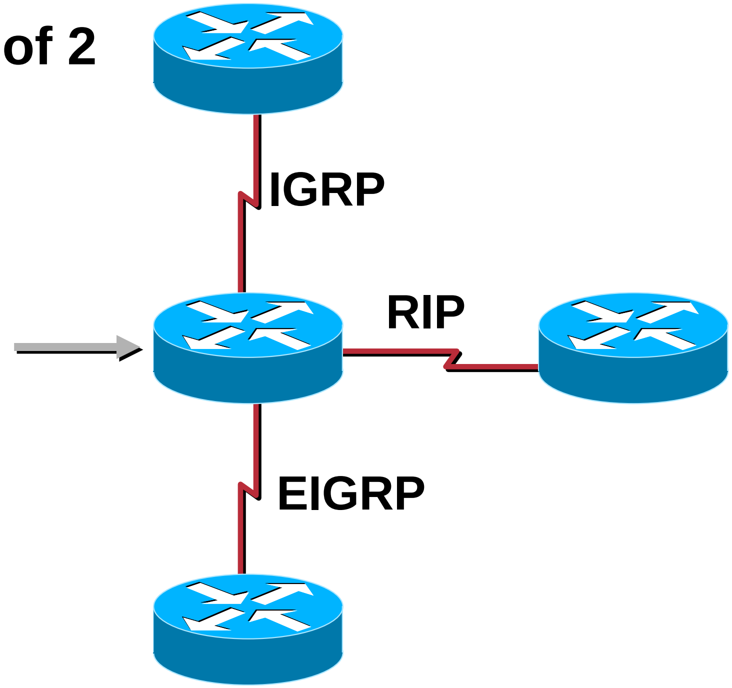
```
router rip
 redistribute igrp 1 metric 1
 redistribute eigrp 3
 default-metric 2
```

RIP/IGRP/EIGRP

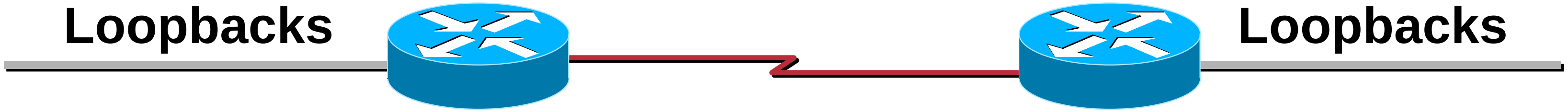
Route Redistribution

Redistribute igrp and eigrp into RIP; Assign Specific igrp Routes a Metric (hop count) of 1, Other igrp Routes a Metric of 3 and eigrp Routes a Metric of 2

```
router rip
 redistribute igrp 1 route-map igrpmetric
 redistribute eigrp 3
 default-metric 2

route-map igrpmetric permit 10
 match ip address 1
 set metric 1
route-map igrpmetric permit 20
 set metric 3

access-list 1 permit 172.16.0.0 0.0.255.255
```



Preparation Suggestions

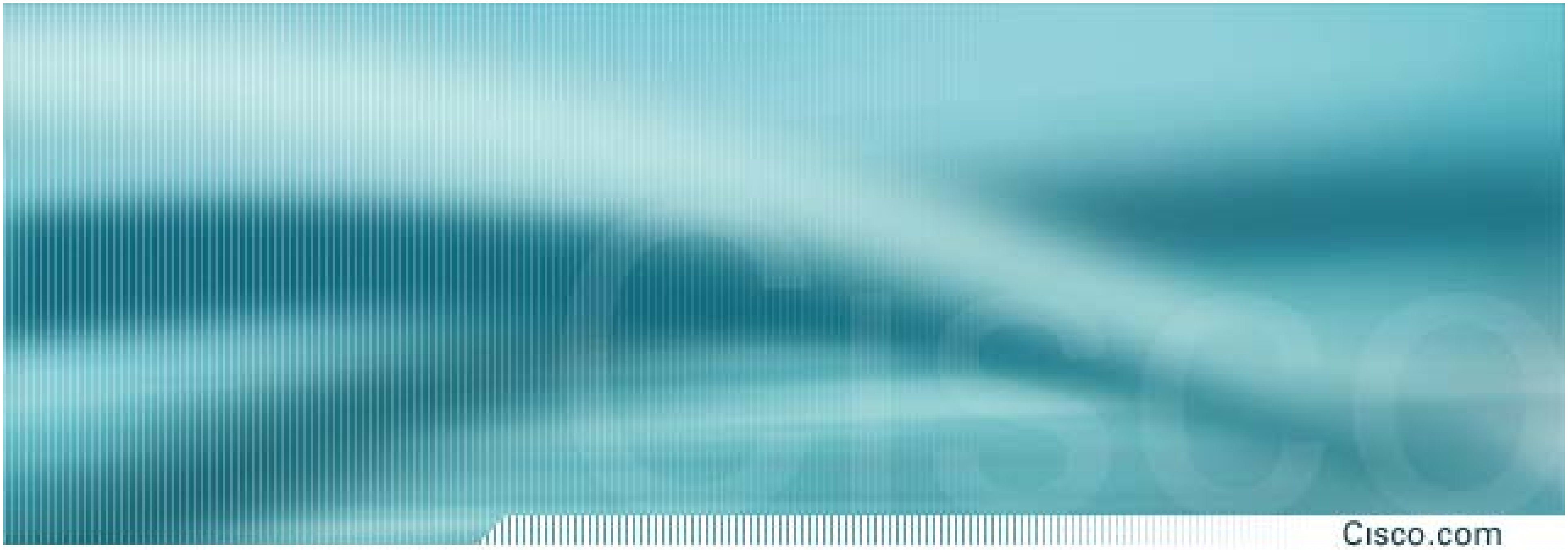


- **With two routers you can practice every command**

References

- Routing TCP/IP Vol. 1 Jeff Doyle, Cisco Press
- EIGRP Network Design Solutions, Ivan Pepelnjak, Cisco Press
- Cisco Documentation

Questions?



Session 4

IP Routing OSPF

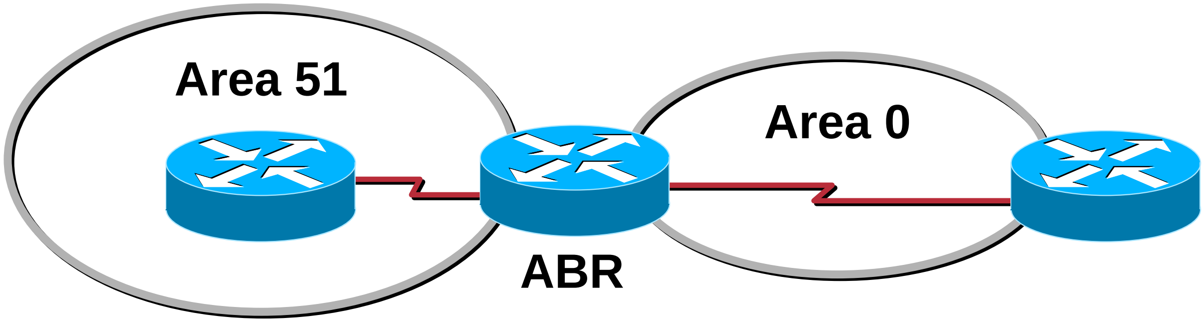
OSPF

- Terminology
- Commands—Router
- Commands—Interface
- Commands—Monitoring
- Preparing for OSPF

Terminology

- **Area Border Router—ABR**

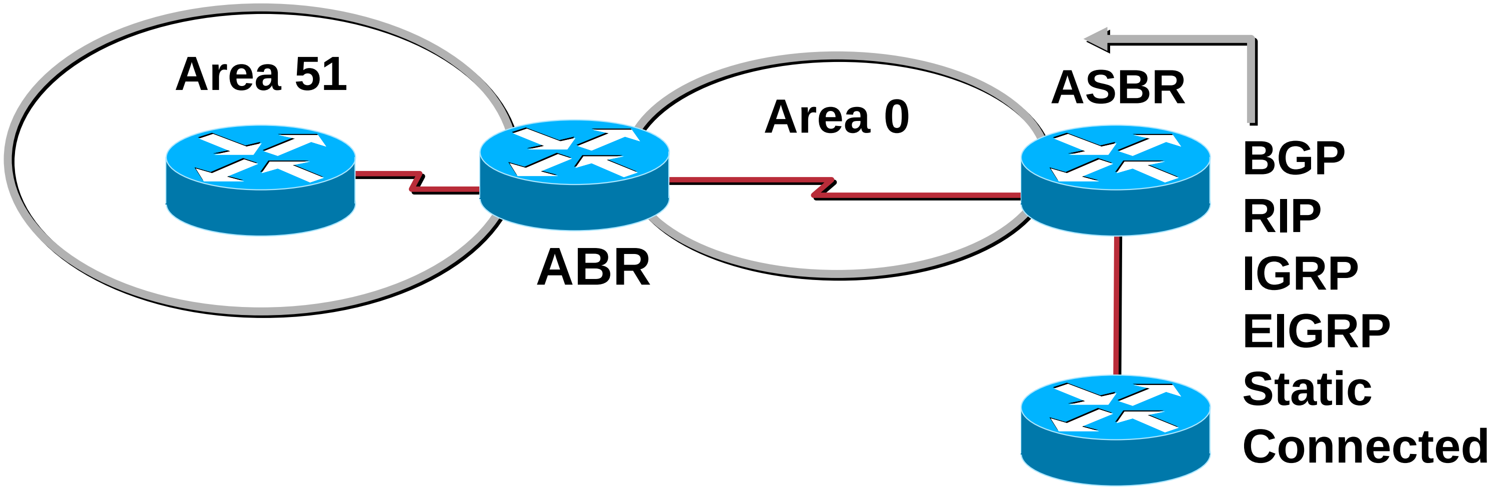
  A router with at least one interface in area 0 and 1 or more interfaces in one or more non-backbone areas



Terminology

- **Autonomous System Boundary Router—ASBR**

  A router with at least one interface in an OSPF area that is redistributing routes from another protocol into OSPF

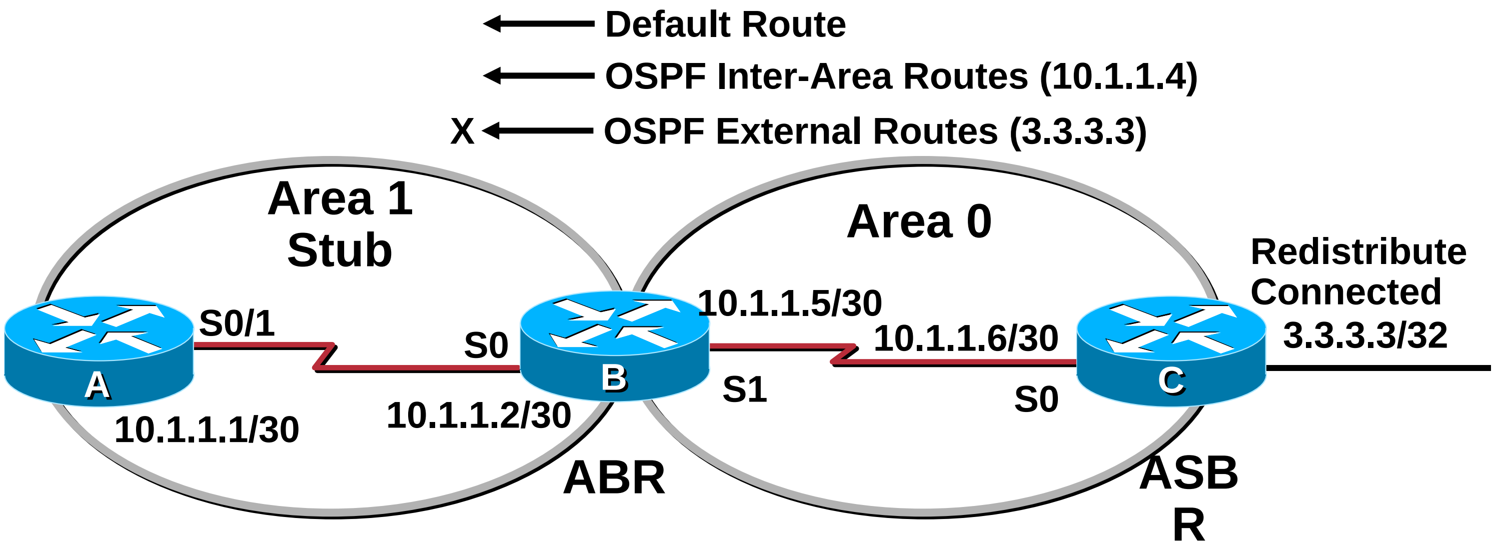


Terminology

Stub Area

Redistributed routes (OSPF external routes or Type 5) are not advertised into a Stub Area. OSPF Inter-area routes are Advertised into a stub area. The ABR will advertise a default into the stub area.

area 1 stub configure on all routers in the area



Default Route

OSPF Inter-Area Routes (10.1.1.4)

X OSPF External Routes (3.3.3.3)

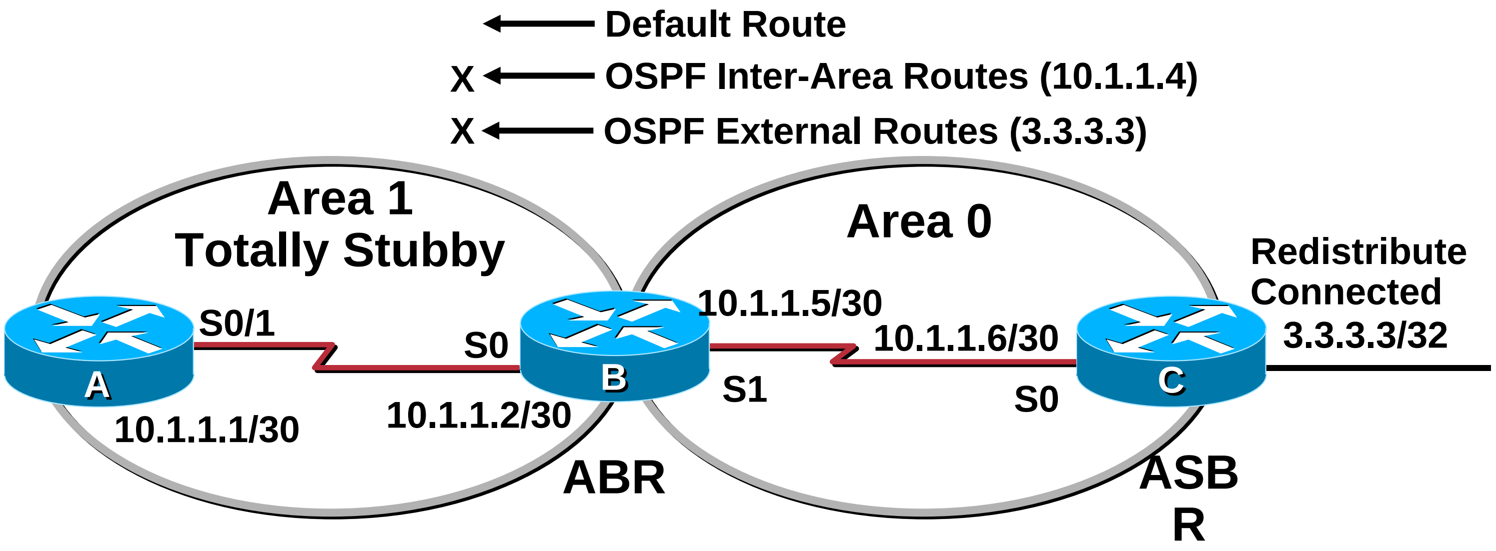
Terminology

Cisco.com

Totally Stubby Area

Redistributed routes (OSPF external routes or Type 5) and OSPF Inter-area routes are not advertised into a Totally Stubby Area. The ABR will advertise a default into the stub area.

area 1 stub no-summary—configure on the ABR

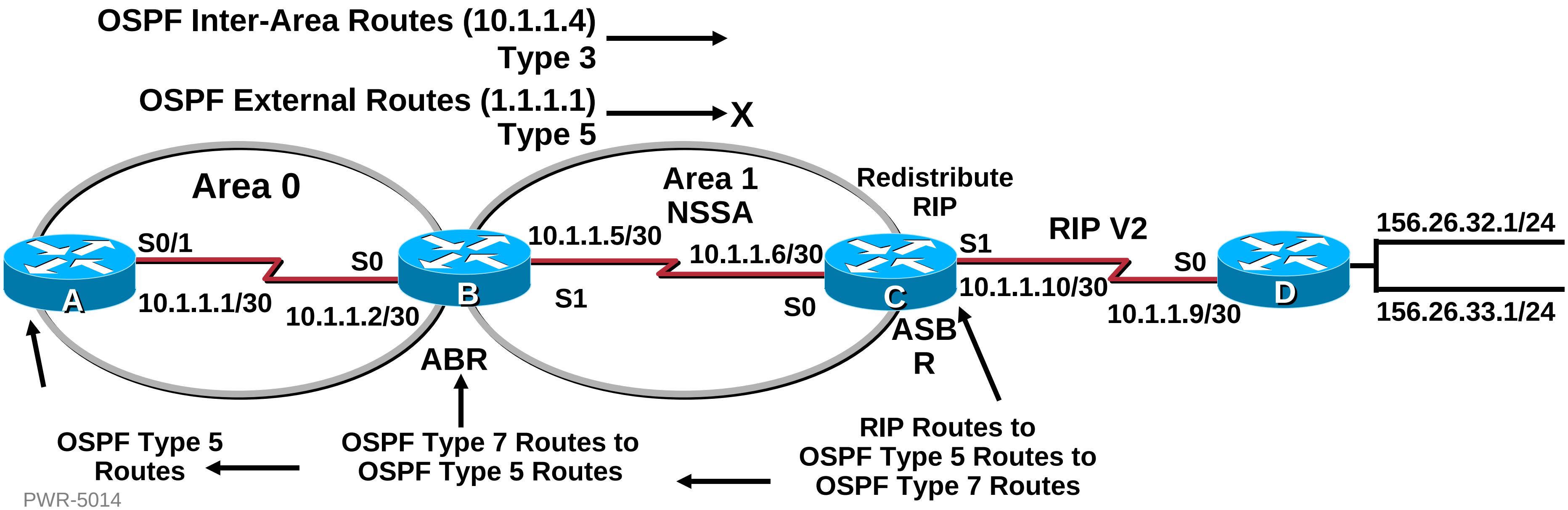


Terminology

Not So Stubby Area—NSSA

Redistributed routes (OSPF external routes or Type 5) are converted to Type 7 at the ASBR. The ABR converts them back to type 5. The ABR will not advertise a default into the stub area.

area 1 nssa—configure on all routers in the area



OSPF Inter-Area Routes (10.1.1.4) Type 3

OSPF External Routes (1.1.1.1) Type 5

OSPF Type 5 Routes

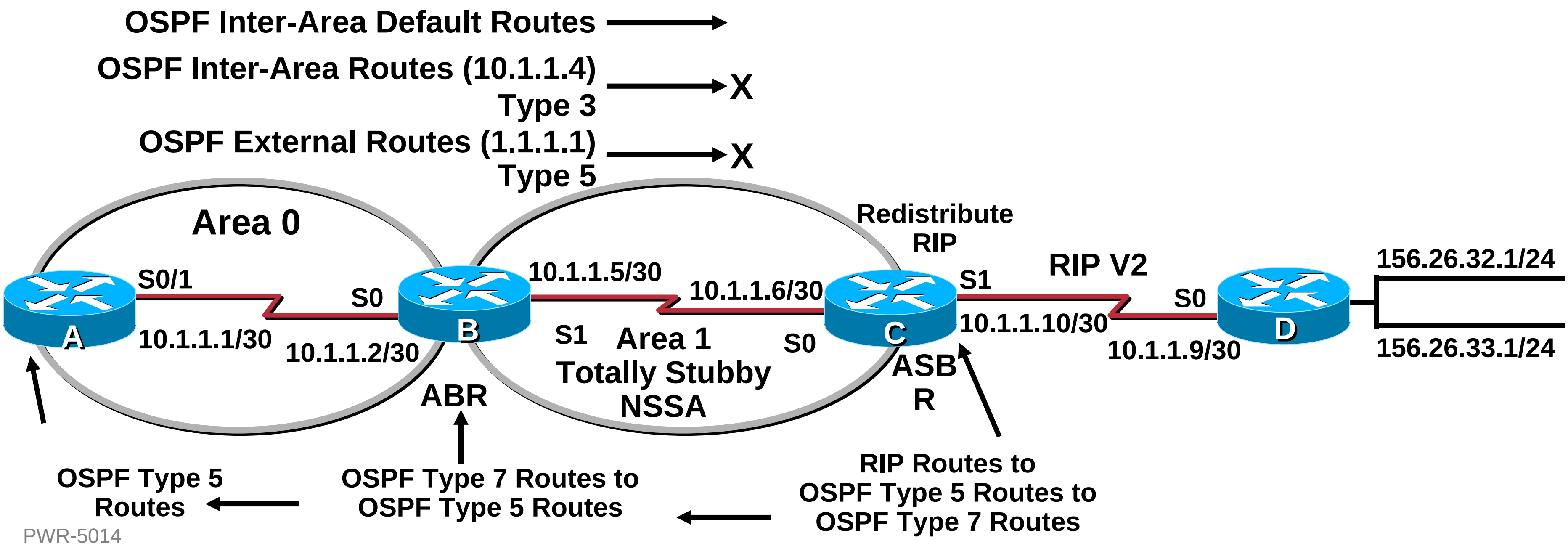
OSPF Type 7 Routes to OSPF Type 5 Routes

RIP Routes to OSPF Type 5 Routes to OSPF Type 7 Routes

Totally Not So Stubby Area—NSSA

Redistributed routes (OSPF external routes or Type 5) are converted to Type 7 at the ASBR. The ABR converts them back to type 5. The ABR will not advertise a default into the stub area. OSPF Inter-area routes are not advertised into the area. The ABR will advertise a default route into the area.

area 1 nssa no-summary—configure on the ABR



OSPF Inter-Area Default Routes →

OSPF Inter-Area Routes (10.1.1.4) Type 3 → X

OSPF External Routes (1.1.1.1) Type 5 → X

Area 0

Redistribute RIP

RIP V2

S0/1

S0

10.1.1.5/30

10.1.1.6/30

S1

S0

156.26.32.1/24

A

B

C

D

10.1.1.1/30

10.1.1.2/30

S1

Area 1 Totally Stubby NSSA

S0

10.1.1.10/30

10.1.1.9/30

156.26.33.1/24

ASBR

ABR

OSPF Type 5 Routes ←

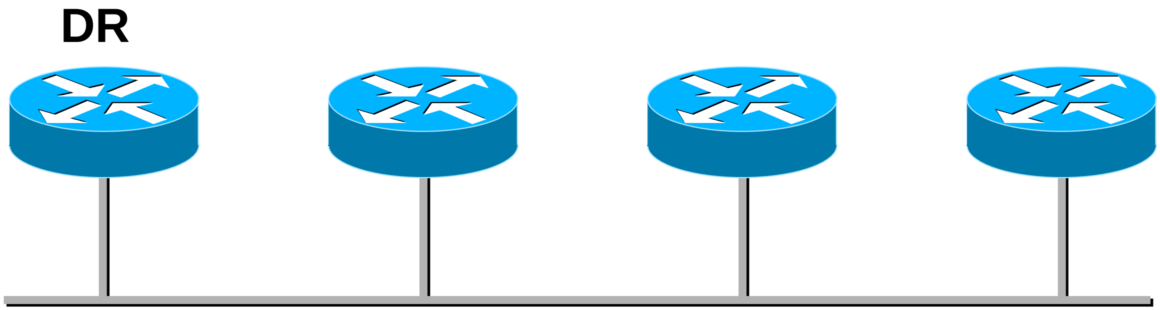
OSPF Type 7 Routes to OSPF Type 5 Routes ←

RIP Routes to OSPF Type 5 Routes to OSPF Type 7 Routes

Terminology

- **Designated Router—DR**

  On a multi-access network, the DR is responsible for distributing LSAs to other attached OSPF routers; DR is selected by highest priority (default = 1), highest loopback address, or highest IP address assigned to a physical interface

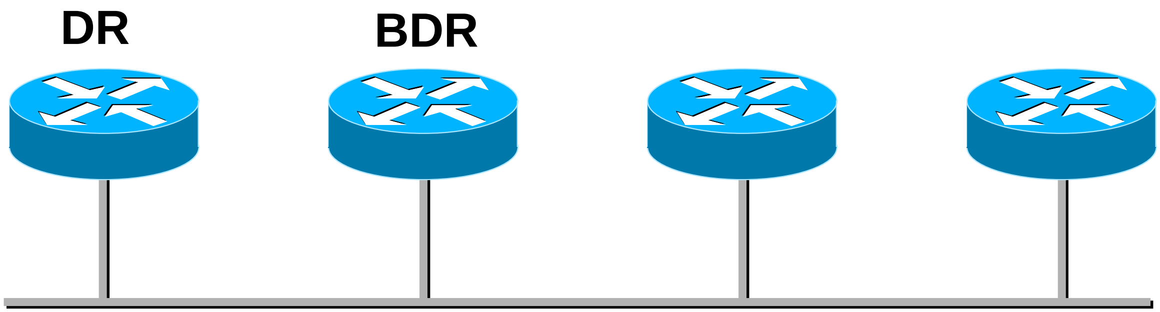


- **Always configure a loopback interface before configuring OSPF**

Terminology

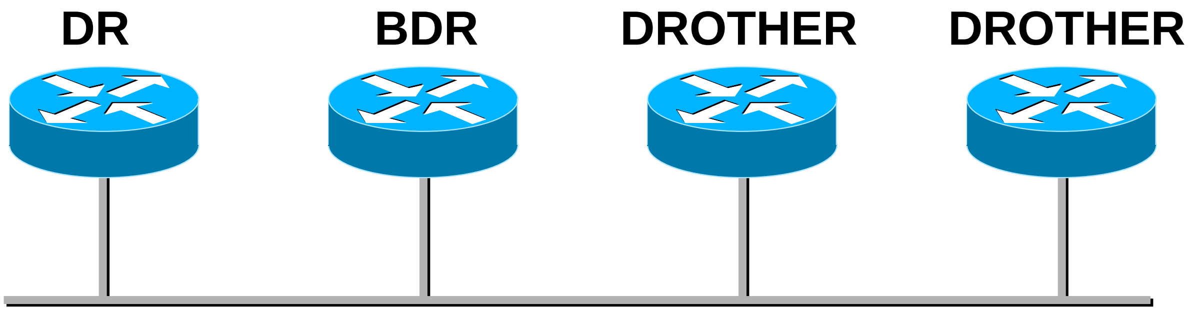
- **Backup Designated Router—BDR**

The BDR will assume the DR role if the DR fails



Terminology

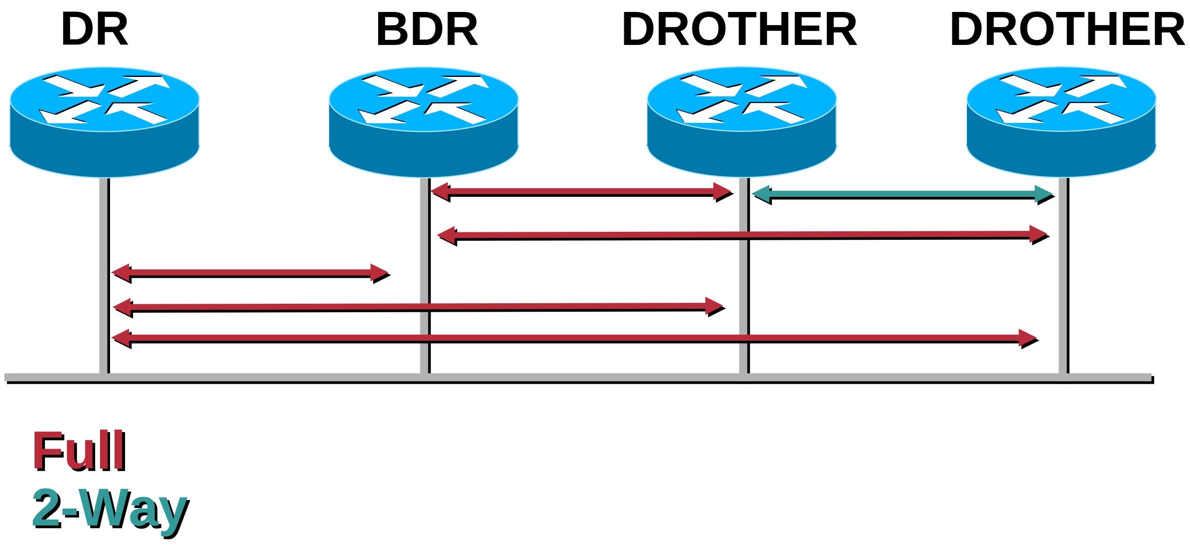
- **DROTHER—Not the DR or BDR**



Terminology

- **Adjacency**

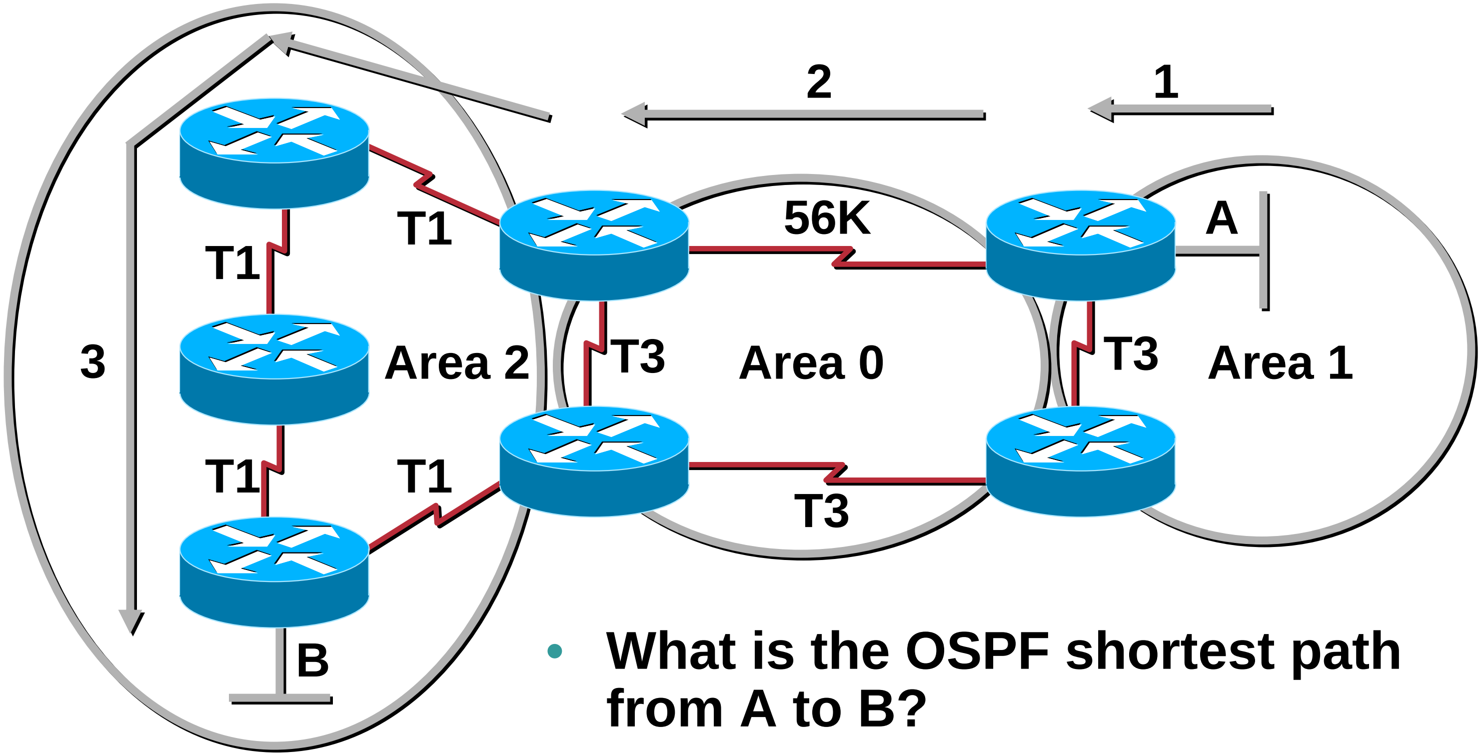
  On a multi-access network, all OSPF routers will become adjacent with the DR and BDR



Terminology

Cisco.com

OSPF Route Selection



- **What is the OSPF shortest path from A to B?**
  1. Shortest path to area 0
  2. Shortest path across area 0 without going through a non-zero-area
  3. Shortest path to B without going through area 0

Commands—Router

Cisco.com

```
Rtr(config)#router ospf 1
Rtr(config-router)#?
Router Configuration Commands:
```

***area	OSPF Area Parameters
**auto-cost	Calculate OSPF Interface Cost According to Bandwidth
default	Set a Command to Its Defaults
*default-information	Control Distribution of Default Information
*default-metric	Set Metric of Redistributed Routes
*distance	Define an Administrative Distance
*distribute-list	Filter Networks in Routing Updates
*ignore	Do Not Complain about Specific Event
*log-adjacency-changes	Log Changes in Adjacency State
*maximum-paths	Forward Packets over Multiple Paths

Importance: ***High **Medium *Low

Commands—Router

```
Rtr(config)#router ospf 1
Rtr(config-router)#?
Router Configuration Commands:
```

**neighbor	Specify a Neighbor Router
***network	Enable Routing on an IP Network
*no	Negate a Command or Set Its Defaults
*passive-interface	Suppress Routing Updates on an Interface
***redistribute	Redistribute Information from Another Routing Protocol
*router-id	Router-id for this OSPF Process
***summary-address	Configure IP Address Summaries
*timers	Adjust Routing Timers
*traffic-share	Algorithm for Computing Traffic Share for Alternate

Importance: ***High **Medium *Low

Commands—Router

Area

```
Rtr(config-router)#area ?
```

<0-4294967295>	OSPF Area ID as a Decimal Value
A.B.C.D	OSPF Area ID in IP Address Format

```
Rtr(config-router)#area 1 ?
```

**Authentication	Enable Authentication
*default-cost	Set the Summary Default-Cost of a NSSA/Stub Area
*nssa	Specify a NSSA Area
***range	Summarize Routes Matching Address/Mask (Border Routers Only)
*stub	Specify a Stub Area
***virtual-link	Define a Virtual Link and its Parameters

Importance: ***High **Medium *Low

Commands—Router

Default-Metric

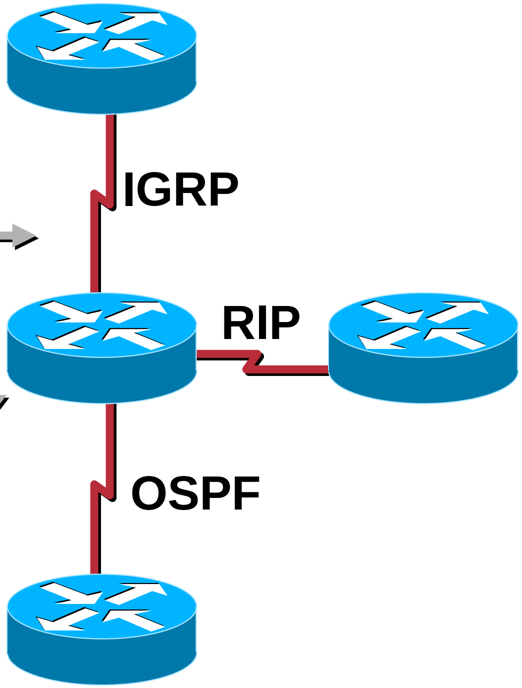
```
Rtr(config-router)#default-metric ?
 <1-4294967295>  Default metric
```

Assign a Cost of 10 to All RIP Routes Redistributed into OSPF

```
router ospf 1
 default metric 10
 redistribute rip subnets
```

Assign a Cost of 20 to All RIP Routes and 10 to Any Other Routes Redistributed into OSPF

```
router ospf 1
 default metric 10
 redistribute rip subnets metric 20
 redistribute igrp 1 subnets
```

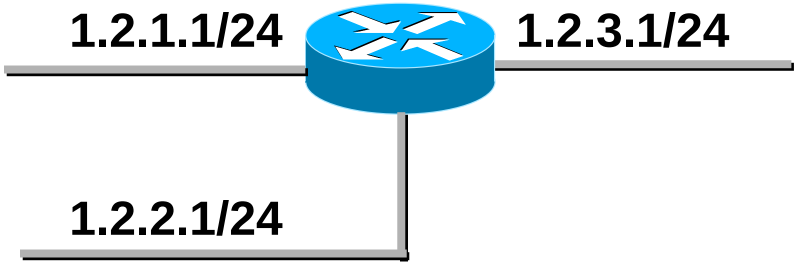


Commands—Router

Network

- The network command is used to determine which interfaces will be enabled for OSPF

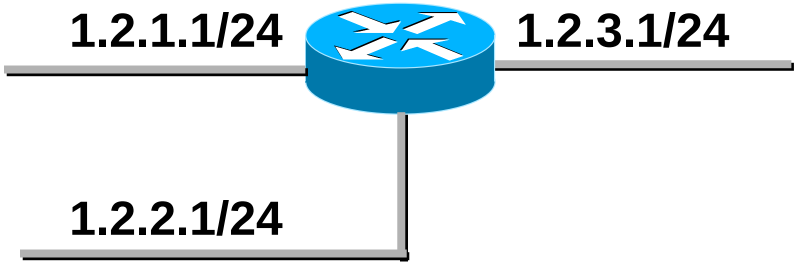
```
network 1.2.1.1        0.0.0.0 area 0
network 1.2.2.1        0.0.0.0 area 1
network 1.2.3.1        0.0.0.0 area 2
```



Commands—Router

Network

```
network 1.2.1.00.0.0.255 area 0
network 1.2.2.00.0.0.255 area 1
network 1.2.3.00.0.0.255 area 2
```

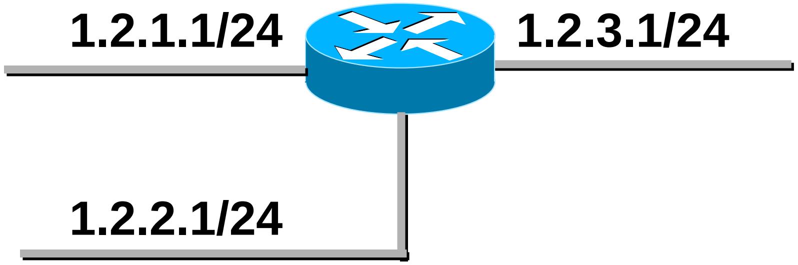


Commands—Router

Cisco.com

Network

network 1.2.0.0 0.0.255.255 area 0



Commands—Router

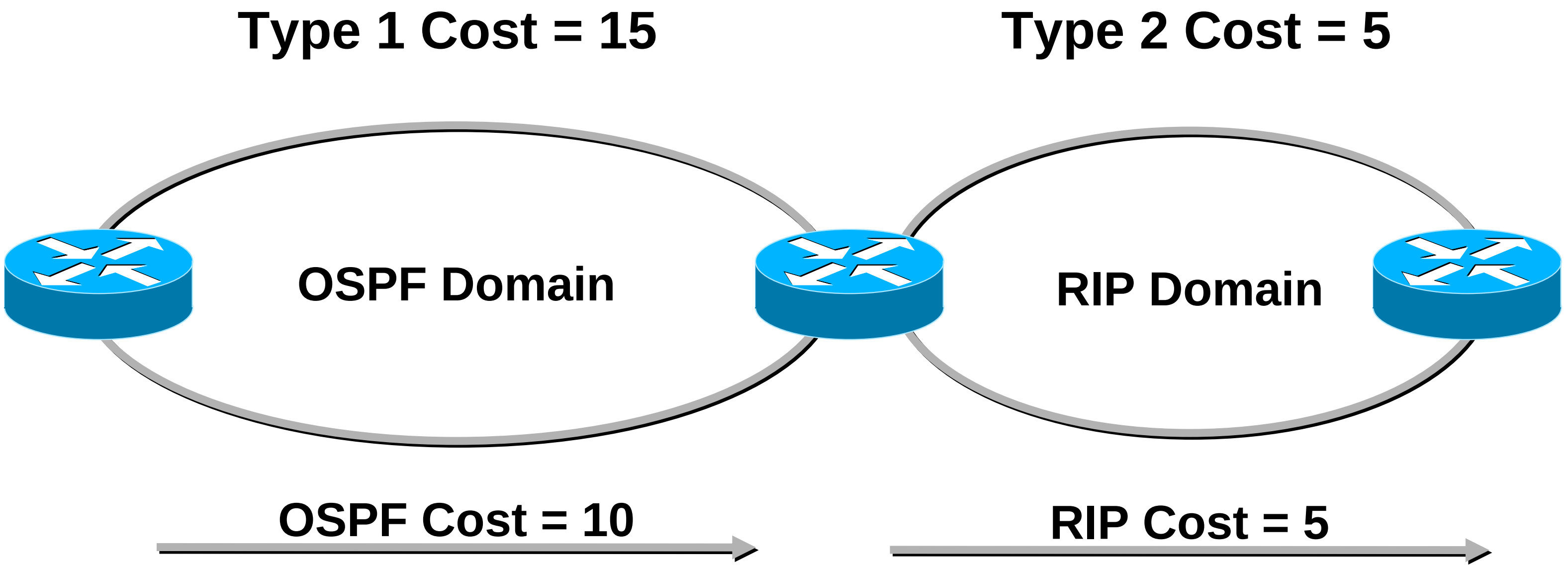
Cost—External Routes

- **By default, redistributed routes have external metric type 2; Type 2 routes have a cost which consists of the external cost only; Type 1 routes include the cost of traversing the OSPF domain**

```
Rtr(config-router)#redistribute rip metric-type ?
  1  Set OSPF External Type 1 metrics
  2  Set OSPF External Type 2 metrics
```

Commands—Router

Cost—External Routes



Type 1 Cost = 15

Type 2 Cost = 5

OSPF Domain

RIP Domain

OSPF Cost = 10

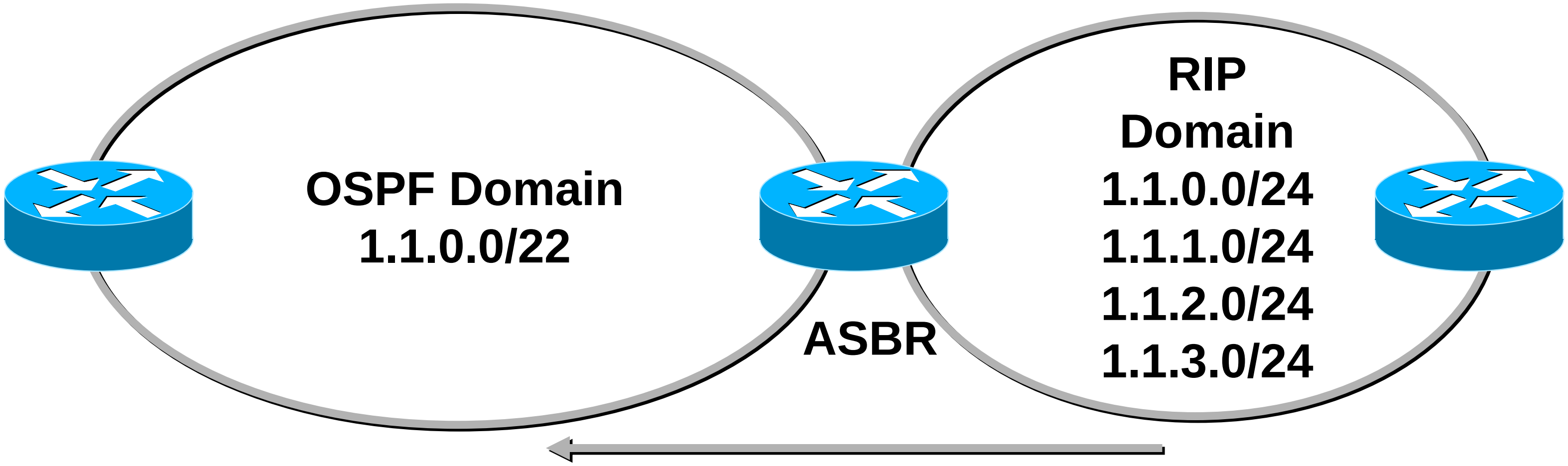
RIP Cost = 5

Commands—Router

Summary-Address

- **Addresses can be summarized into OSPF on an ASBR**

summary-address 1.1.0.0 255.255.252.0

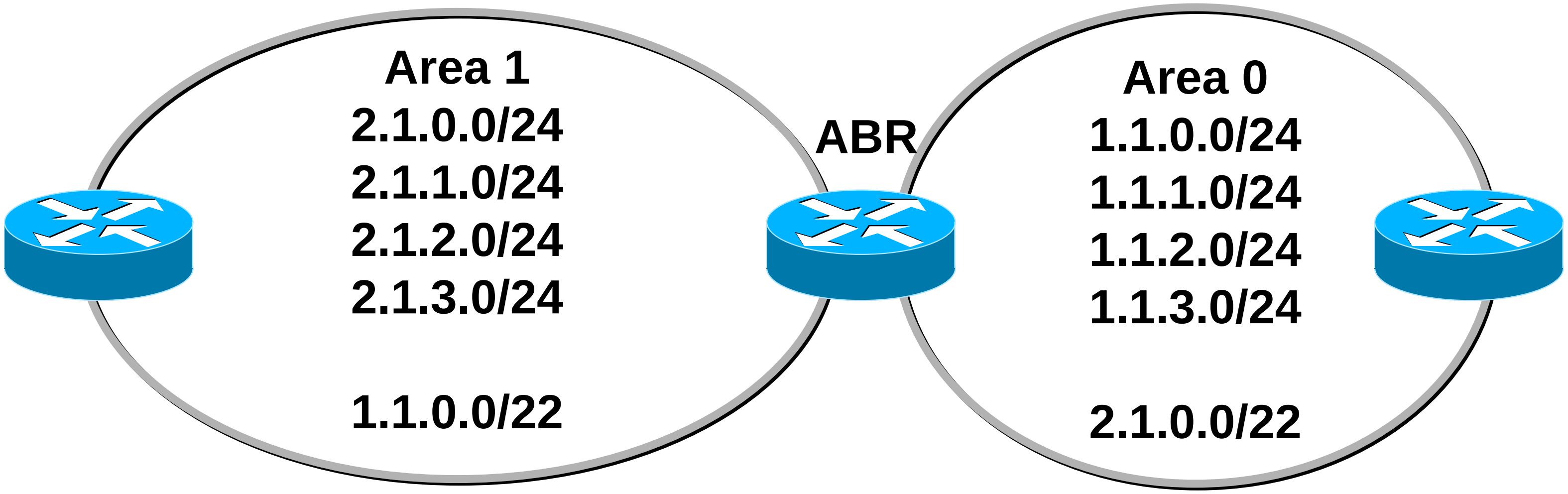


Commands—Router

Range

- **Addresses can be summarized on an ABR into area 0 or from area 0**

```
area 1 range 2.1.0.0 255.255.252.0
area 0 range 1.1.0.0 255.255.252.0
```



Area 1
2.1.0.0/24
2.1.1.0/24
2.1.2.0/24
2.1.3.0/24

1.1.0.0/22

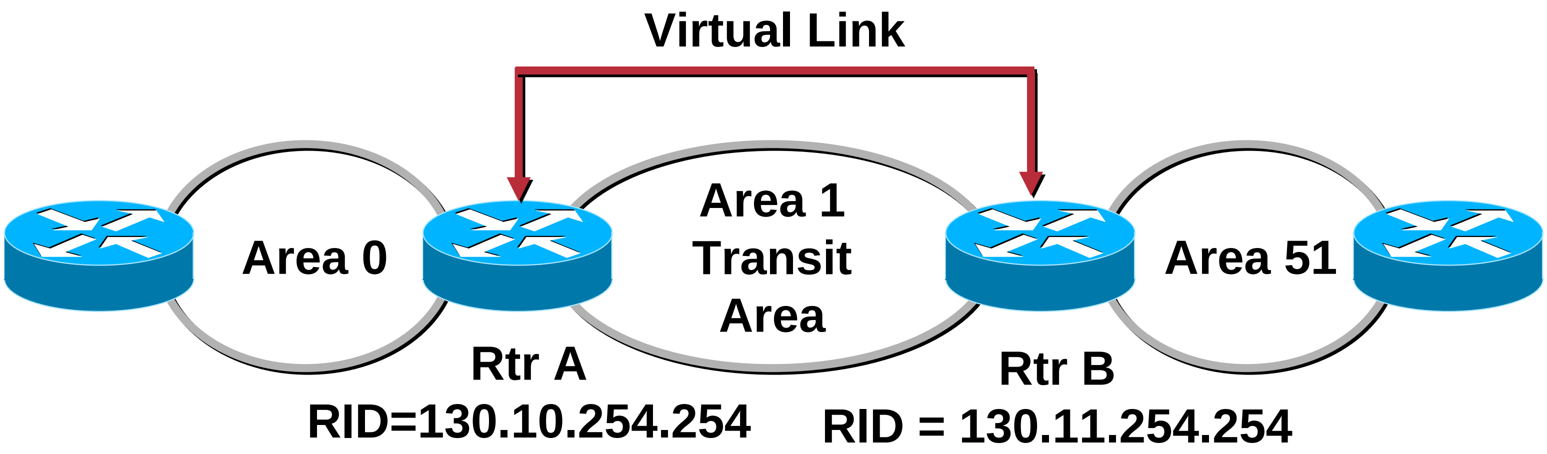
ABR

Area 0
1.1.0.0/24
1.1.1.0/24
1.1.2.0/24
1.1.3.0/24

2.1.0.0/22

Commands—Router

Virtual Link



Rtr A

```
router ospf 1
 area 1 virtual-link 130.11.254.254
```

Rtr B

```
router ospf 1
 area 1 virtual-link 130.10.254.254
```

Commands—Router

Auto Cost

- **OSPF interfaces have a cost equal to 100,000,000/Bandwidth**

  Fast Ethernet = 100,000,000/100,000,000 = 1

  Ethernet = 100,000,000/10,000,000 = 10

  T1 = 100,000,000/1,544,000 = 65

- **The auto-cost command is used to change the default of 100,000,000; changing the default affects the cost of every OSPF interface on the router**

- **Rtr(config-router)#auto-cost reference-bandwidth? <1-4294967> The reference bandwidth in terms of Mbits per second**

Commands—Interface

```
Rtr(config-if)#ip ospf ?
```

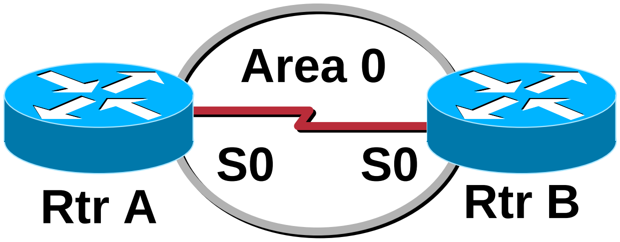
***authentication-key	Authentication Password (Key)
**cost	Interface Cost
*database-filter	Filter OSPF LSA during Synchronization and Flooding
*dead-interval	Interval after which a Neighbor Is Declared Dead
***demand-circuit	OSPF Demand Circuit
*hello-interval	Time between HELLO Packets
***message-digest-key	Message Digest Authentication Password (Key)
***network	Network Type
***priority	Router Priority
*retransmit-interval	Time between Retransmitting Lost Link State Advertisements
*transmit-delay	Link State Transmit Delay

Importance: ***High **Medium *Low

Commands—Interface

Authentication—Clear Text

- Authentication requires router and interface commands; Router command is used to enable authentication for an area and the interface command is used to enable authentication on an interface

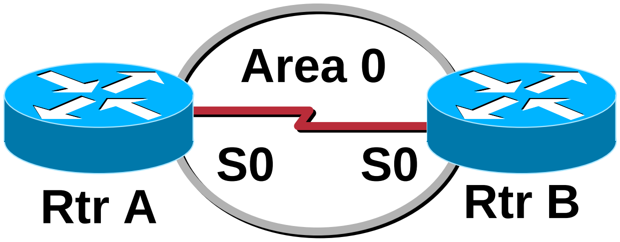


```
Rtr A
interface serial 0
 ip ospf authentication-key cisco
!
router ospf 1
 area 0 authentication
```

```
Rtr B
interface serial 0
 ip ospf authentication-key cisco
!
router ospf 1
 area 0 authentication
```

Commands—Interface

Authentication—Message Digest

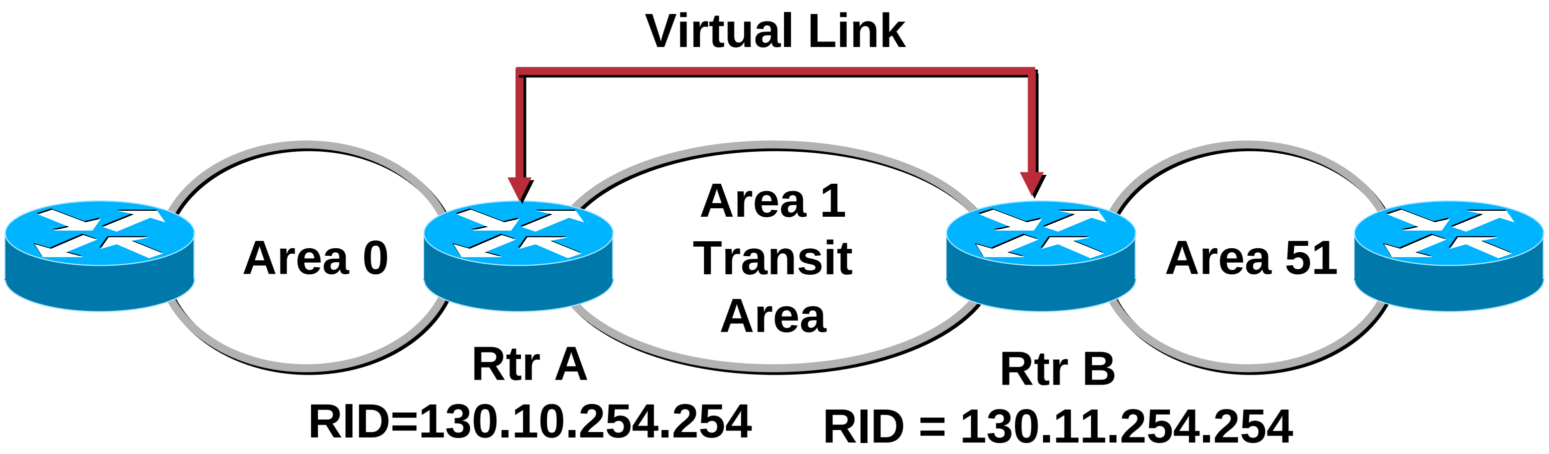


```
Rtr A
interface serial 0
ip ospf message-digest-key 1 md5 cisco
!
router ospf 1
 area 0 authentication message-digest
```

```
Rtr B
interface serial 0
ip ospf message-digest-key 1 md5 cisco
!
router ospf 1
 area 0 authentication message-digest
```

Commands—Interface

Authentication—Virtual Link



Virtual Link

Area 0

Area 1
Transit
Area

Area 51

Rtr A
RID=130.10.254.254

Rtr B
RID = 130.11.254.254

Rtr A

```
router ospf 1
 area 1 virtual-link 130.11.254.254 authentication-key cisco
 area 0 authentication
```

Rtr B

```
router ospf 1
 area 1 virtual-link 130.10.254.254 authentication-key cisco
 area 0 authentication
```

Authentication—Can Be Applied per Interface or Virtual Link (Cisco IOS 12.x)

Interface

ip ospf authentication
ip ospf authentication-key *password*

ip ospf authentication message-digest
ip ospf message-digest *key-id* **md5** *password*

ip ospf authentication null

Virtual Link

area *area-id* **virtual-link** *router-id* **authentication authentication-key** *password*

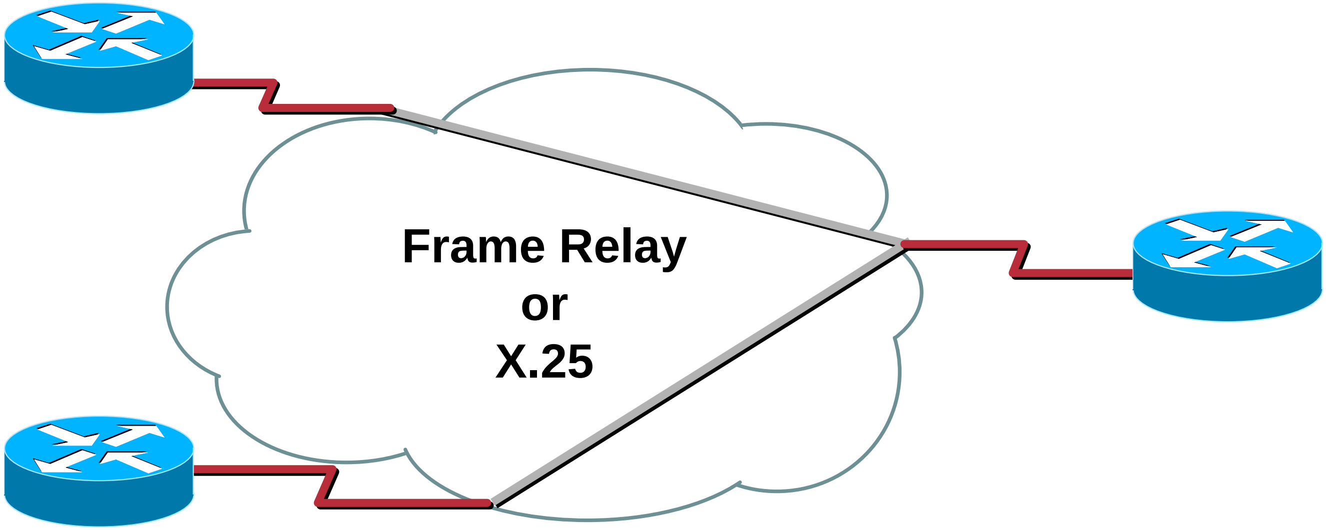
area *area-id* **virtual link** *router-id* **authentication message–digest**
area *area-id* **virtual link** *router-id* **message-digest-key** *key-id* **md5** *password*

area *area-id* **virtual-link** *router-id* **authentication null**

Commands—Interface

Cisco.com

Non-Broadcast Multi-Access (NBMA) Network



Pvcs Can Be on Same Subnet or on Different Subnets

Practice and Understand the Effect of OSPF Network Types

ip ospf network point-to-multipoint (Hello = 30, Dead = 120)
Ip ospf network point-to-point (Hello = 10, Dead = 40)
ip ospf network broadcast (Hello = 10, Dead = 40)

Commands—Monitoring

Show

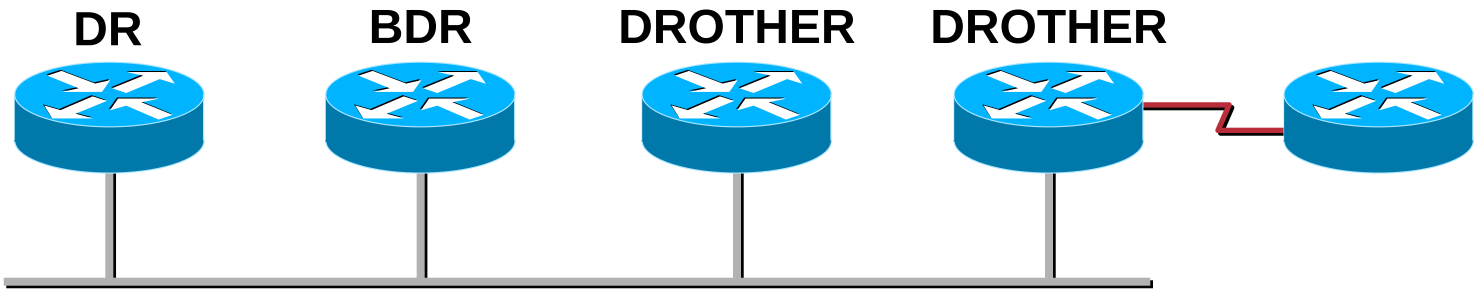
```
Rtr#show ip ospf ?
```

*** <1-4294967295>	Process ID Number
border-routers	Border and Boundary Router Information
database	Database Summary
flood-list	Link State Flood List
**interface	Interface Information
***neighbor	Neighbor List
request-list	Link State Request List
retransmission-list	Link State Retransmission List
summary-address	Summary-Address Redistribution Information
***virtual-links	Virtual Link information
|	Output Modifiers
<cr>	

Importance: ***High **Medium *Low

Commands—Monitoring

Show IP OSPF Neighbor



show ip ospf neighbor

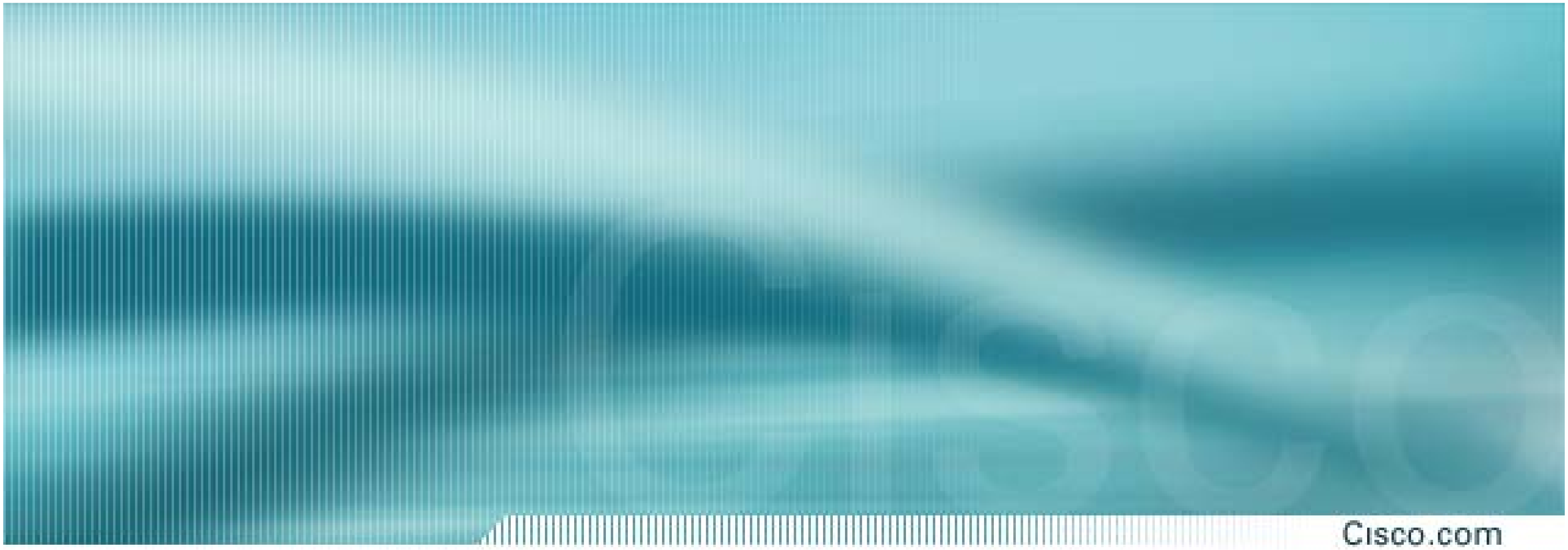
Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.254	1	2WAY/DROTHER	00:00:35	1.1.2.1	Ethernet0
1.1.3.254	1	FULL/BDR	00:00:39	1.1.2.2	Ethernet0
1.1.4.254	1	FULL/DR	00:00:37	1.1.2.3	Ethernet0
1.1.5.254	1	FULL/---	00:00:36	1.1.6.1	Serial0

Preparation Suggestions

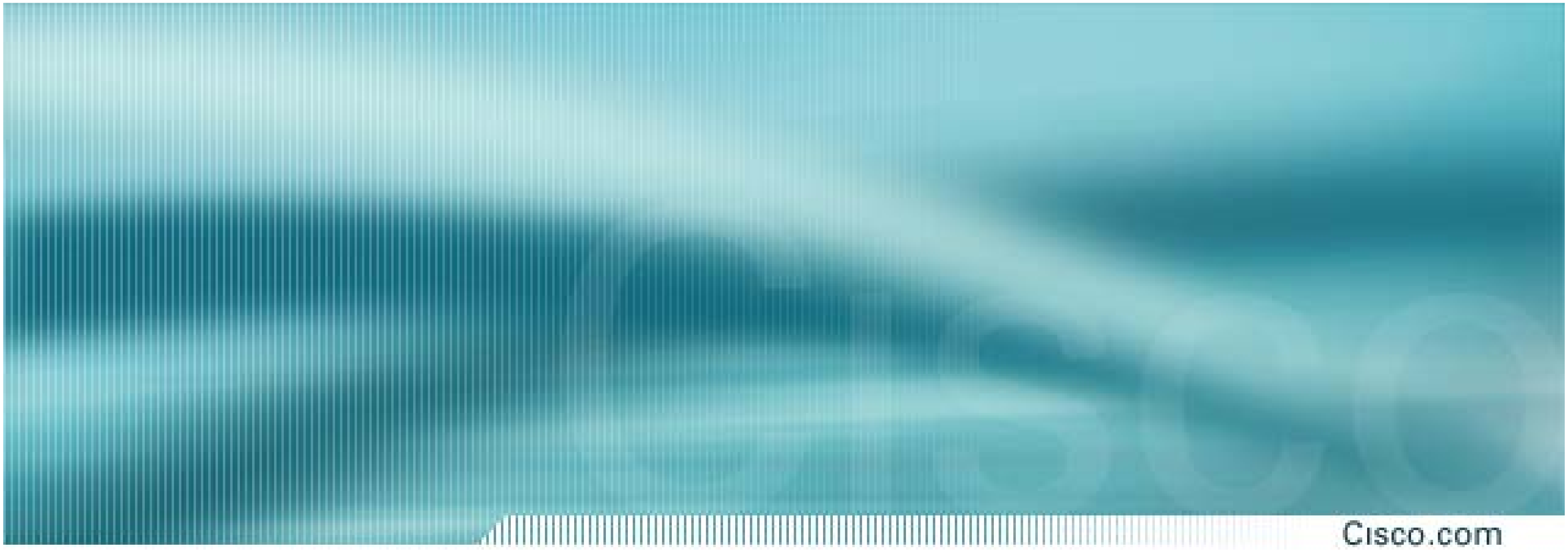
- Practice every OSPF command
- Practice OSPF over Frame Relay

References

- **Cisco OSPF Command and Configuration Handbook**
  William R. Parkhurst, Cisco Press
- **OSPF Network Design Solutions**
  Thomas M. Thomas, Cisco Press
- **Cisco Documentation**



Questions?



Session 5

IP Routing

BGP/ISIS

BGP

BGP

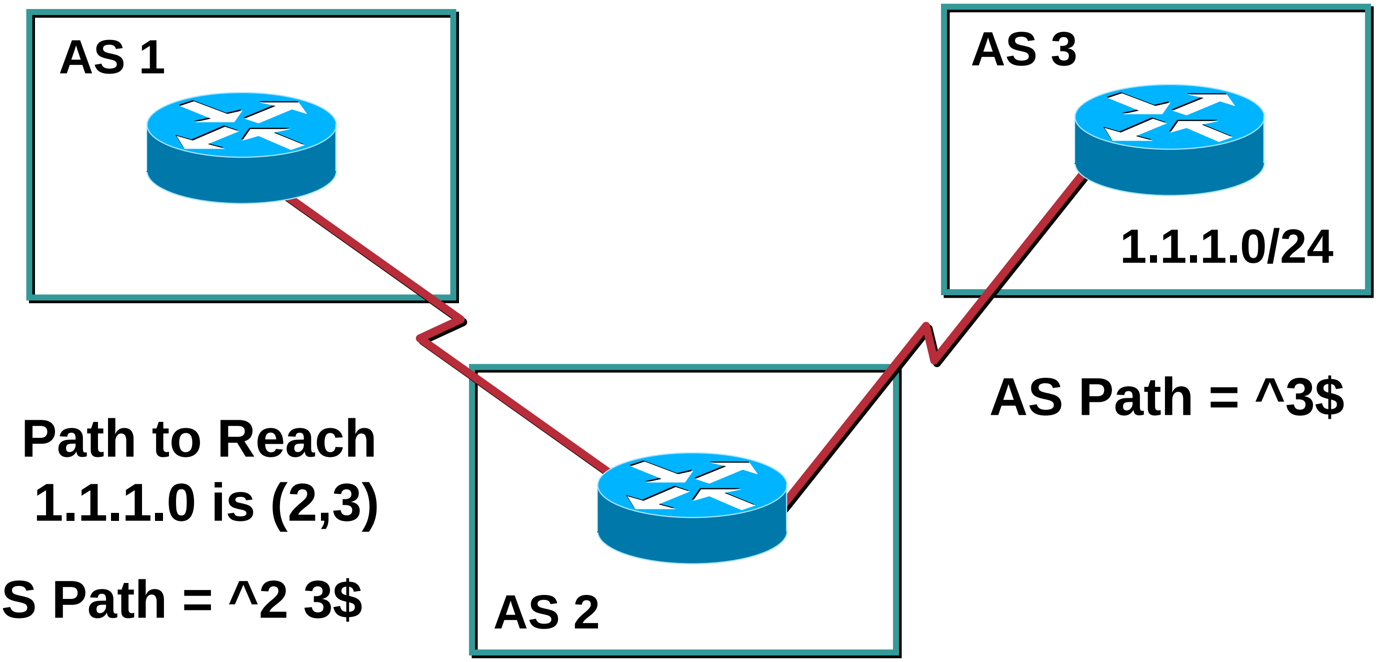
- BGP Attributes
- Commands—Router
- Debugging
- Preparing for BGP

BGP Attributes

Cisco.com

AS Path

- AS Path attribute—the list of AS numbers that a route has traversed to reach a destination



BGP Attributes

Origin

- IGP

  Network Layer Reachability Information (NLRI) is interior to the originating AS

- EGP

  NLRI is learned via EBGP

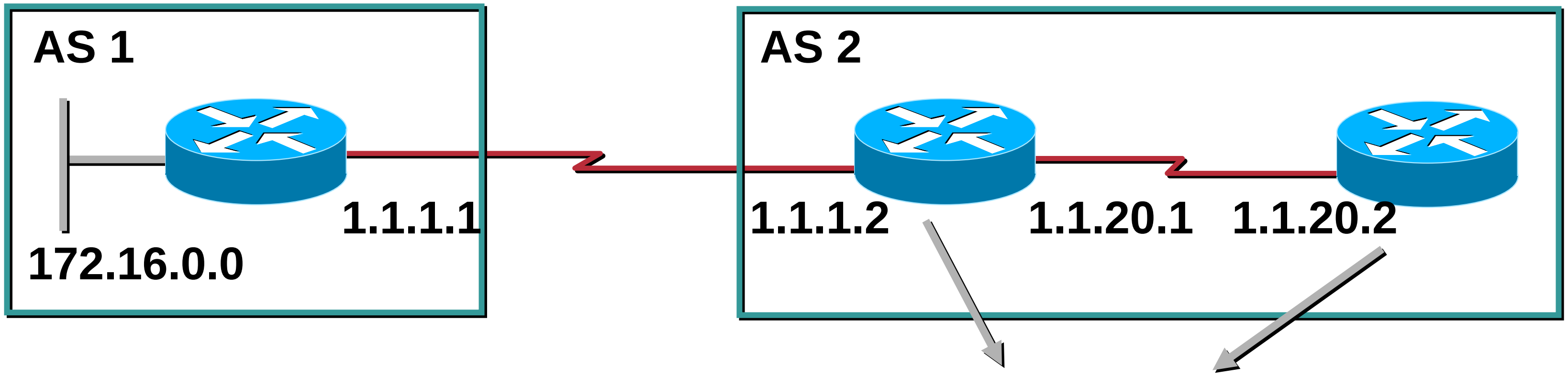
- Incomplete

  NLRI is unknown; usually when redistributing static into BGP

BGP Attributes

Next Hop

- The next hop IP address that is used to reach a destination
- For EBGP, the next hop is the IP address specified in the neighbor command
- For IBGP, the EBGP next hop information is carried into IBGP

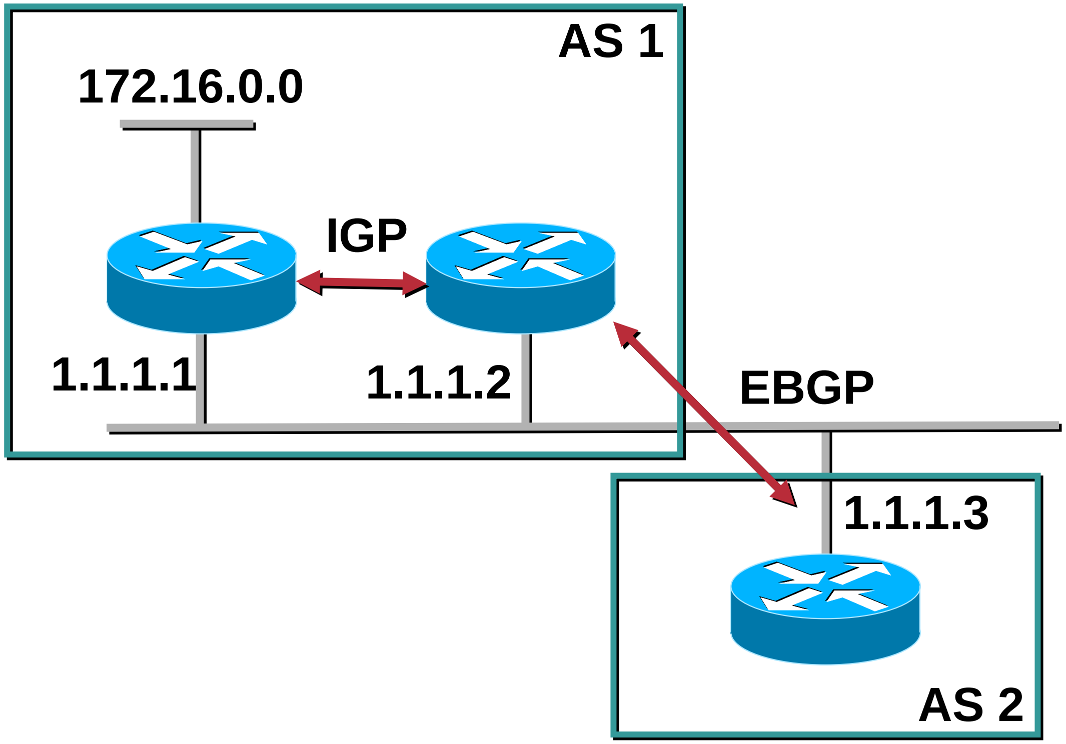


172.16.0.0
Next hop = 1.1.1.1

BGP Attributes

Cisco.com

Next Hop—Multi-Access Networks

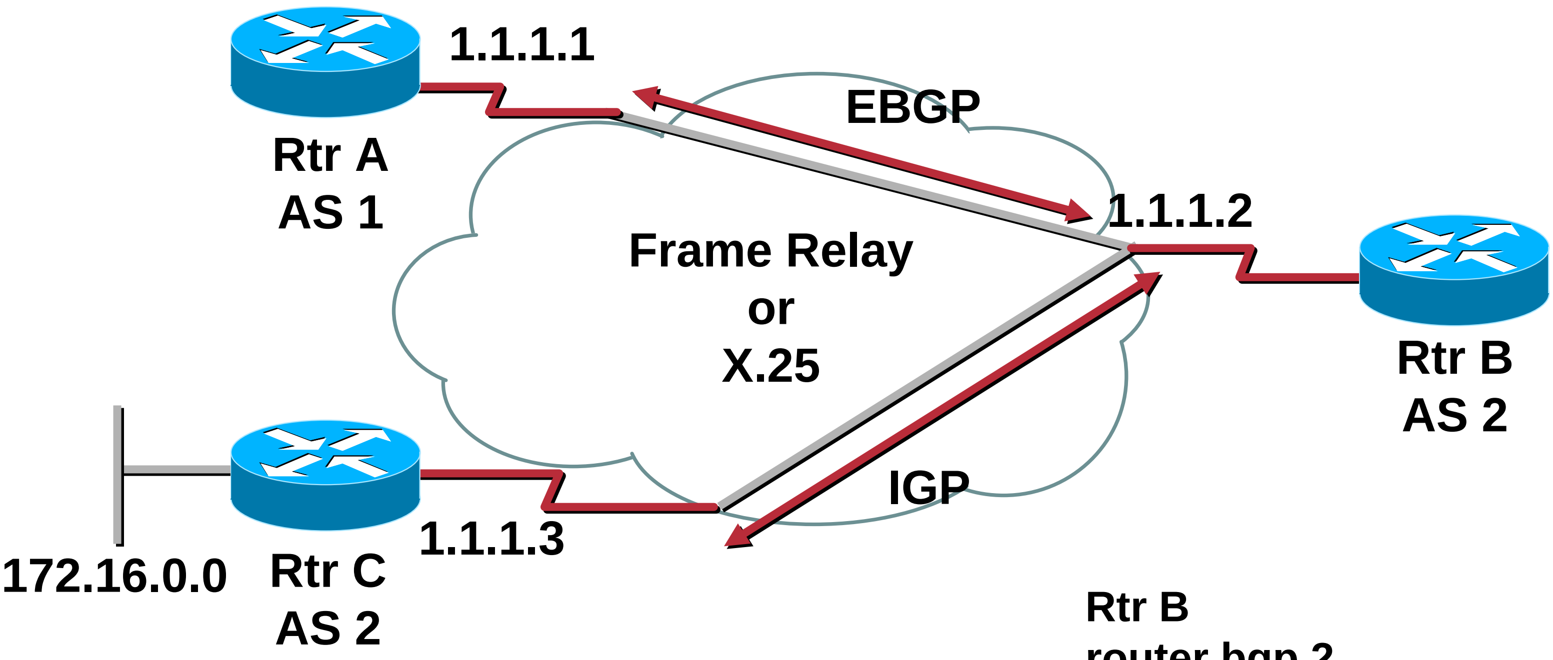


172.16.0.0
Nexthop = 1.1.1.1

BGP Attributes

Next Hop—NBMA Networks

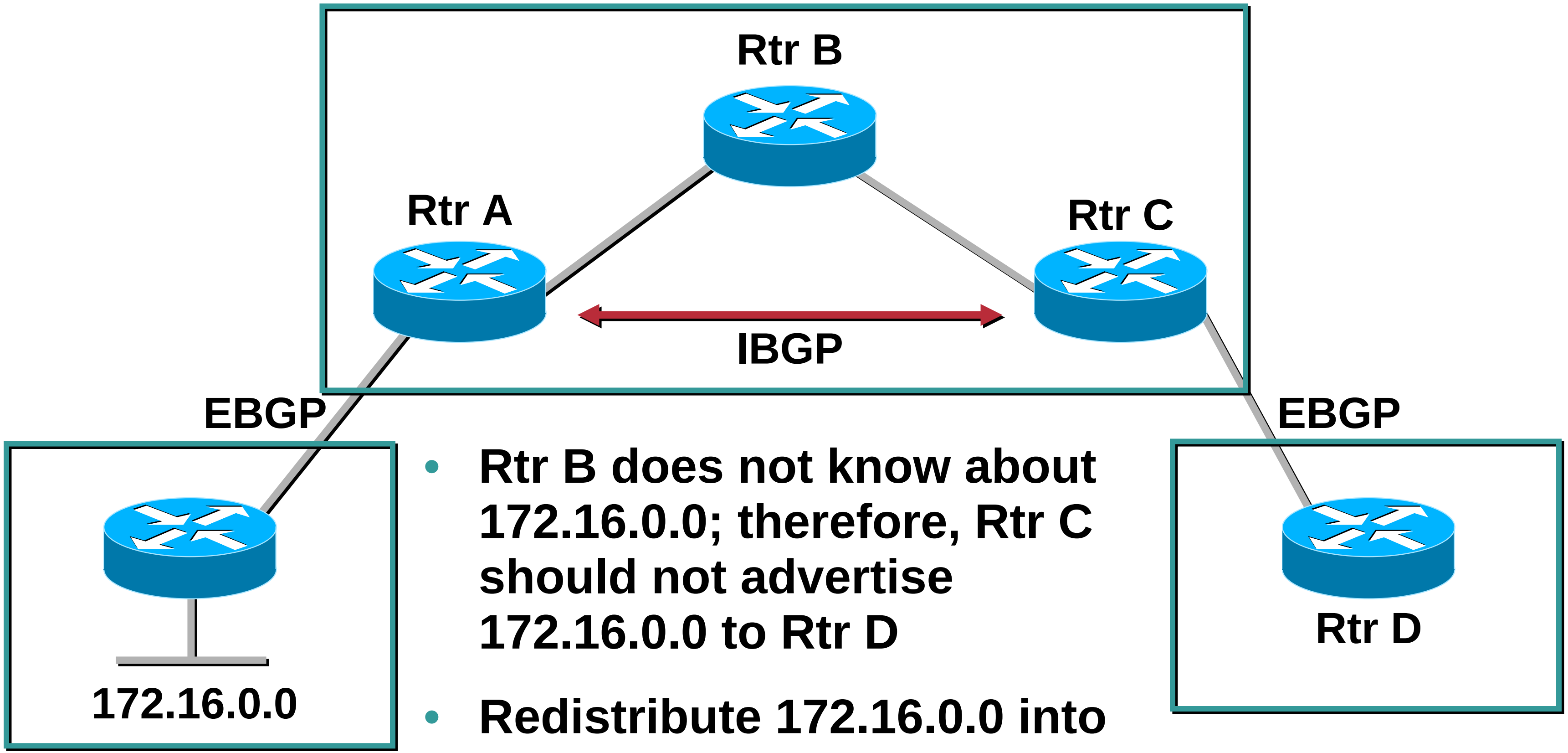
Nexthop to 172.16.0.0 is 1.1.1.3—Needs to be 1.1.1.2



```
Rtr B
router bgp 2
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 next-hop-self
```

BGP Attributes

Synchronization

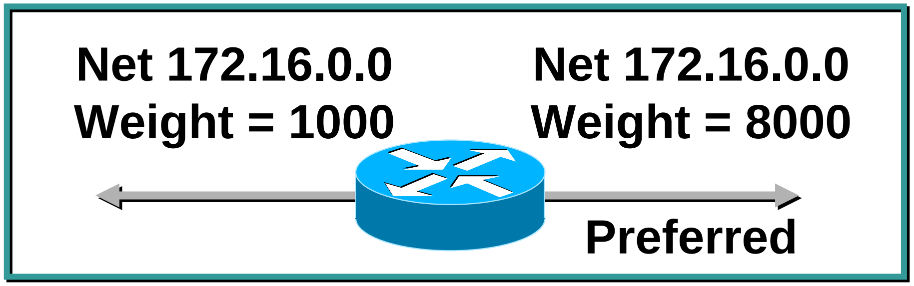


- Rtr B does not know about 172.16.0.0; therefore, Rtr C should not advertise 172.16.0.0 to Rtr D
- Redistribute 172.16.0.0 into IGP or use a full IBGP mesh

BGP Attributes

Weight

- A Cisco defined attribute which is used for path selection; the weight is assigned locally and is not propagated in routing updates



Net 172.16.0.0
Weight = 1000

Net 172.16.0.0
Weight = 8000

Preferred

Value: 0 - 65535
Default Value: 32768
Higher value is preferred

Adjust by neighbor

```
neighbor 1.1.1.1 weight <0 - 65535>
```

Adjust using a filter-list

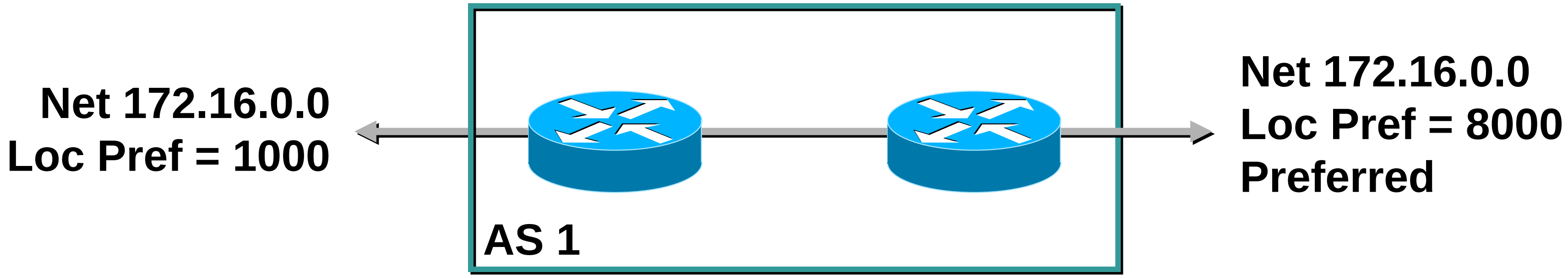
```
neighbor 1.1.1.1 filter-list 5 weight 300
…
ip as-path access-list 5 permit ^100$
```

Adjust using a route map

```
neighbor 1.1.1.1 route-map adjwt in
...
route-map adjwt permit 10
 match as-path 5
 set weight 300
route-map adjwt permit 20
 set weight 200
```

BGP Attributes

Local Preference



- Signals which path is preferred to exit the AS and is exchanged among all BGP speakers in the AS; Local Preference is not exchanged between ASs
- Value: 0-4294967295
  - Default value: 100
  - Higher value is preferred
- Set on all updates to routers in the AS
- bgp default local-preference 200

BGP Attributes

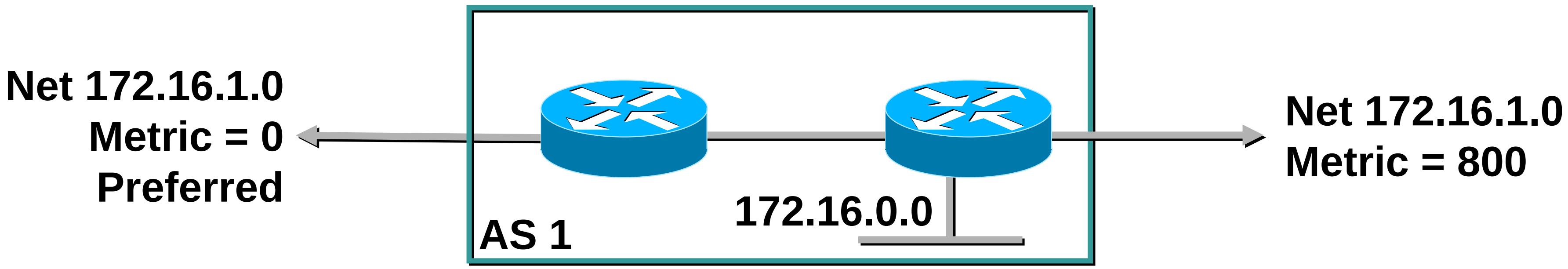
Local Preference

Set based on AS destination

```
neighbor 1.1.1.1 route-map localpref in
…
route-map localpref permit 10
 match as-path 8
 set local-preference 800
route-map local-pref permit 20
 set local-preference 350

ip as-path 8 permit ^2$
```

BGP Attributes

Metric



- Also known as the Multi—Exit-Discriminator (MED); Metric is used as a suggestion to other ASs about the preferred path into the AS; exchanged between ASs
- Value: 0–4294967295
- Default value: 0
- Lower value is preferred

BGP Attributes

Metric

Set based on AS destination

```
neighbor 1.1.1.1 route-map setmed out
…
route-map setmed permit 10
 match as-path 8
 set metric 800
route-map setmed permit 20
 set metric 350
…
ip as-path 8 permit ^2$
```

Set based on IP Address

```
neighbor 1.1.1.1 route-map setmed out
...
route-map setmed permit 10
 match ip address 1
 set metric 800
route-map setmed permit 20
 set metric 350
...
access-list 1 permit 172.16.1.0 0.0.0.255
```

BGP Attributes

Community

- Used to group destinations and apply routing decisions according to community; by default, not sent to any peers
- Value: 0–4,294,967,200 or 0:0–65535:65535
- Well known communities

no-export	(Do not advertise to EBGP peers)
no-advertise	(Do not advertise to any peer)

- To send community values to a peer use

  neighbor 1.1.1.1 send-community

BGP Attributes

Setting the Community Value

```
router bgp 1
 neighbor 10.1.1.1 remote-as 2
 neighbor 10.1.1.1 send-community
 neighbor 10.1.1.1 route-map setcomm {in | out}
!
access-list 1 permit 172.16.1.0 0.0.0.255
!
route-map setcomm permit 10
 match ip address 1
 set community 65546 (or 1:10) {additive}
```

BGP Attributes

Viewing the Community Value—Old Format

```
rtrA#sh ip bgp 172.16.1.0
BGP routing table entry for 172.16.1.0/24, version 7
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  172.10.2.2 172.10.6.6
  254
    10.1.1.1 from 10.1.1.1 (199.172.15.254)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 65546
```

BGP Attributes

Viewing the Community Value—New Format

ip bgp-community new-format (global configuration)

```
rtrA#sh ip bgp 172.16.1.0
BGP routing table entry for 172.16.1.0/24, version 7
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  172.10.2.2 172.10.6.6
  254
    10.1.1.1 from 10.1.1.1 (199.172.15.254)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 1:10
```

BGP Route Selection

1. Ignore a route if the next hop is not known
2. Ignore IBGP routes that are not synchronized
3. Prefer the route with the largest weight
4. Prefer the route with the largest local preference
5. Prefer the route that was locally originated

BGP Route Selection

6. Prefer the route with the shortest AS path; if using bgp bestpath as-path ignore then skip this step: When using the as-set option for aggregated routes then the as_set counts as 1 regardless of the number of AS entries in the set; confederation sub AS numbers are not used to determine the AS-path length
7. 7. Prefer the route with the lowest origin (IGP < EGP < Incomplete)
8. 8. Prefer the route with the lowest MED; this comparison is only between routes advertised by the same external AS

BGP Route Selection

9. Prefer EBGP routes to IBGP routes
10. Prefer the route with the nearest IGP neighbor
11. Prefer the oldest route
12. Prefer the path received from the router with the lowest router ID

Commands—Router

Router Configuration Commands:

***aggregate-address	Configure BGP Aggregate Entries
*auto-summary	Enable Automatic Network Number Summarization
*bgp	BGP Specific Commands
default	Set a Command to Its Defaults
*default-information	Control Distribution of Default Information
*default-metric	Set Metric of Redistributed Routes
*distance	Define an Administrative Distance
+++distribute-list	Filter Networks in Routing Updates
exit	Exit From Routing Protocol Configuration Mode
help	Description of the Interactive Help System

Importance: ***High **Medium *Low

+++ - Do Not Use with BGP

Use neighbor x.x.x.x distribute-list {in|out}

Commands—Router

Router Configuration Commands:

*maximum-paths	Forward Packets over Multiple Paths
***neighbor	Specify a Neighbor Router
**network	Specify a Network to Announce via BGP
no	Negate a Command or Set Its Defaults
***redistribute	Redistribute Information from Another Routing Protocol
+++summary-address	Configure IP Address Summaries
*synchronization	Perform IGP Synchronization
*table-map	Map External Entry Attributes into Routing Table
*timers	Adjust Routing Timers
+++traffic-share	Algorithm for Computing Traffic Share for Alternate Routes

Importance: ***High **Medium *Low

+++ - Do Not Use with BGP

Commands—Router

Cisco.com

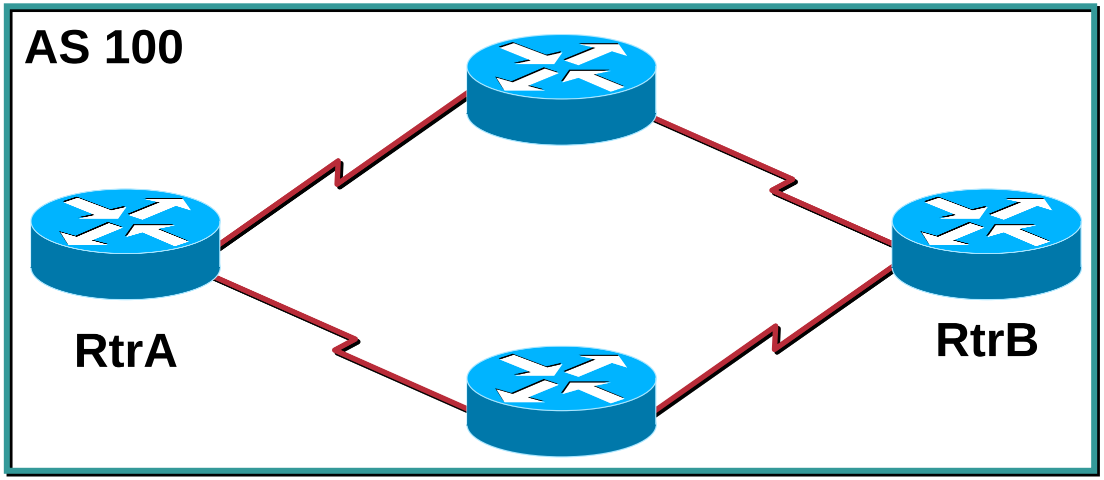
BGP and Loopback Interfaces

RtrA

```
interface loopback0
 ip address 1.1.1.254 255.255.255.255
!
Router bgp 100
 neighbor 1.1.2.254 remote-as 100
 neighbor 1.1.2.254 update-source loopback0
```

RtrB

```
interface loopback0
ip address 1.1.2.254 255.255.255.255
!
router bgp 100
 neighbor 1.1.1.254 remote-as 100
 neighbor 1.1.1.254 update-source loopback0
```



Commands—Router

Network

Used to tell BGP which networks to advertise to neighbors. Unlike IGPs, the network command is not used to determine which interfaces will be active for the protocol. Networks must be in the IP routing table in order for them to be advertised.

```
router bgp 100
 neighbor x.x.x.x remote-as Y
 network 172.16.0.0
```

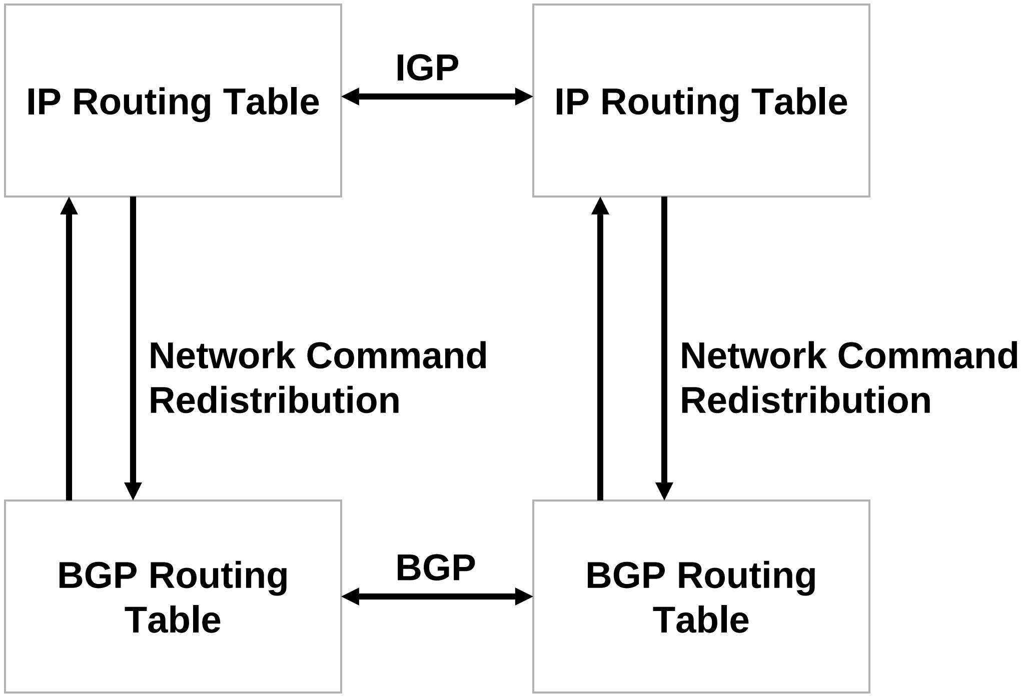
If auto-summary is on then a specific route from 172.16.0.0 must be in the routing table. If auto-summary is off then the prefix 172.16.0.0/16 must be in the IP routing table.

```
network 172.17.1.0 mask 255.255.255.0
```

Must be an exact match in the IP routing table.

Commands—Router

Address Aggregation



IP Routing Table

IGP

IP Routing Table

Network Command
Redistribution

Network Command
Redistribution

BGP Routing
Table

BGP

BGP Routing
Table

BGP Will Advertise
and Aggregate only if
at Least One Specific
Route Exists in the
BGP Routing Table

Commands—Router

Address Aggregation

Assume networks 1.1.0.0/24 and 1.1.1.0/24 are in the IP routing table either directly connected, learned by an IGP, or by EBGP.

Advertise 1.1.0.0/24, 1.1.1.0/24, and 1.1.0.0/23

```
router bgp 1
 network 1.1.0.0 mask 255.255.255.0 (not needed if routes learned
 network 1.1.1.0 mask 255.255.255.0  from BGP or via redistribution)
 aggregate-address 1.1.0.0 255.255.254.0
```

Commands—Router

Cisco.com

Address Aggregation

Assume networks 1.1.0.0/24 and 1.1.1.0/24 are in the IP routing table either directly connected, learned by an IGP, or by BGP.

Advertise 1.1.0.0/23 only

```
router bgp 1
 network 1.1.0.0 mask 255.255.255.0 (not needed if routes learned
 network 1.1.1.0 mask 255.255.255.0  from BGP or via redistribution)
 aggregate-address 1.1.0.0 25 255.255.254.0 summary-only
```

Commands—Router

Cisco.com

Address Aggregation

Assume networks 1.1.0.0/24 and 1.1.1.0/24 are in the IP routing table either directly connected, learned by an IGP, or by EBGP.

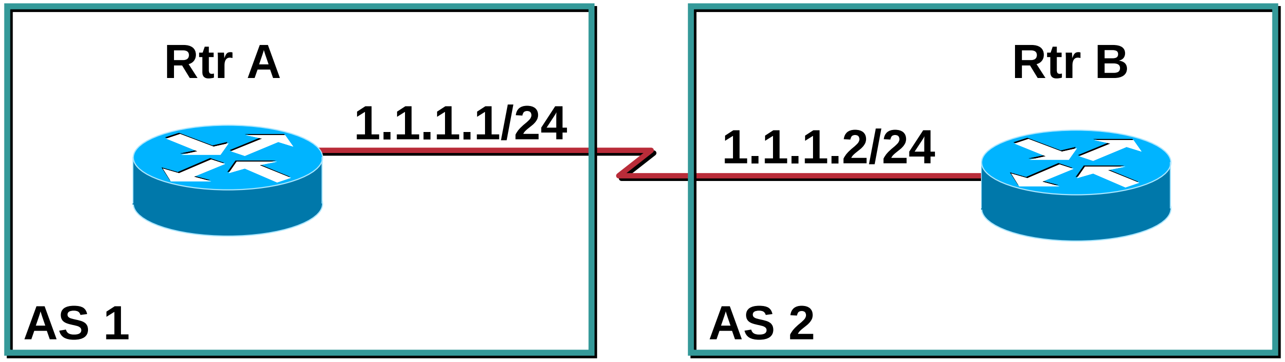
Advertise 1.1.0.0/24 and 1.1.0.0/23 (aggregate and 1 specific route)

```
router bgp 1
 network 1.1.0.0 mask 255.255.255.0
 network 1.1.1.0 mask 255.255.255.0
 aggregate-address 1.1.0.0 255.255.254.0 suppress-map specific
…
access-list 1 permit 1.1.1.0 0.0.0.255
…
route-map specific permit 10  (permit 1.1.1.0 to be suppressed)
 match ip address 1
```

Commands—Router

Cisco.com

Route Filtering



- Filter networks in incoming or outgoing BGP updates based on IP address

Rtr A

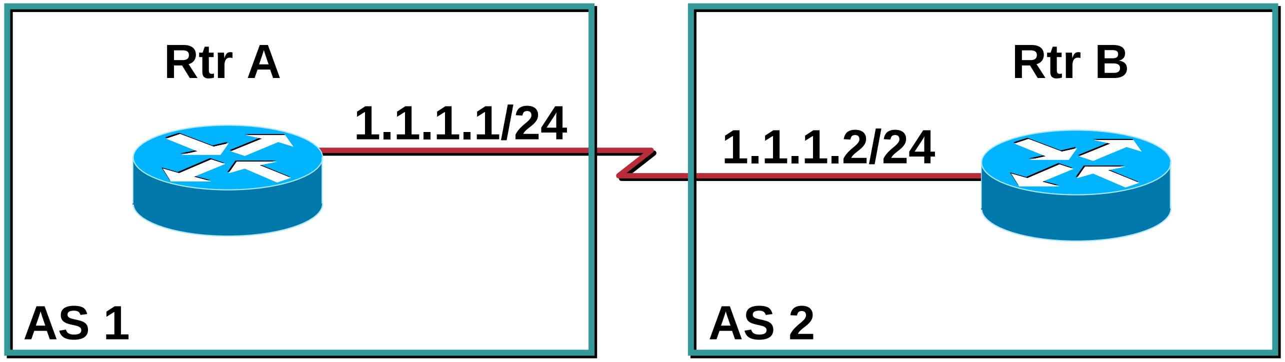
```
router bgp 1
 neighbor 1.1.1.2 distribute-list 1 in

access-list 1 permit 172.16.0.0 0.0.255.255
```

Rtr B

```
router bgp 2
 neighbor 1.1.1.1 distribute-list 2 out

access-list 2 permit 130.15.8.0 0.0.0.255
```

Commands—Router

Route Filtering



- Path Filtering—Filter networks in incoming or outgoing BGP updates based on AS path information

Rtr A

```
router bgp 1
 neighbor 1.1.1.2 filter-list 1 in
…
ip as-path access-list 1 deny ^2$
(deny routes belonging to AS 2)
ip as-path access-list 1 permit .*
```

Rtr B

```
router bgp 2
 neighbor 1.1.1.1 filter-list 2 out
...
ip as-path access-list 2 permit ^$
(allow routes from this AS only)
```

Commands—Router

Route Maps

- Route maps can be used to set BGP parameters (MED, Weight, Local Preference, AS path, etc.)
- Route maps cannot be used to filter incoming updates based on an IP address (Cisco IOS version 11.1 and earlier)

Commands—Router

Route Maps

```
neighbor 1.1.1.1 route-map demo in
…
route-map demo permit 10
 match   as-path       Match BGP AS Path List
         community     Match BGP Community List
         interface     Match First Hop Interface of Route
         ip            IP Specific Information
         length        Packet Length
         metric        Match Metric of Route
         route-type    Match Route-Type of Route
         tag           Match Tag of Route
```

Commands—Router

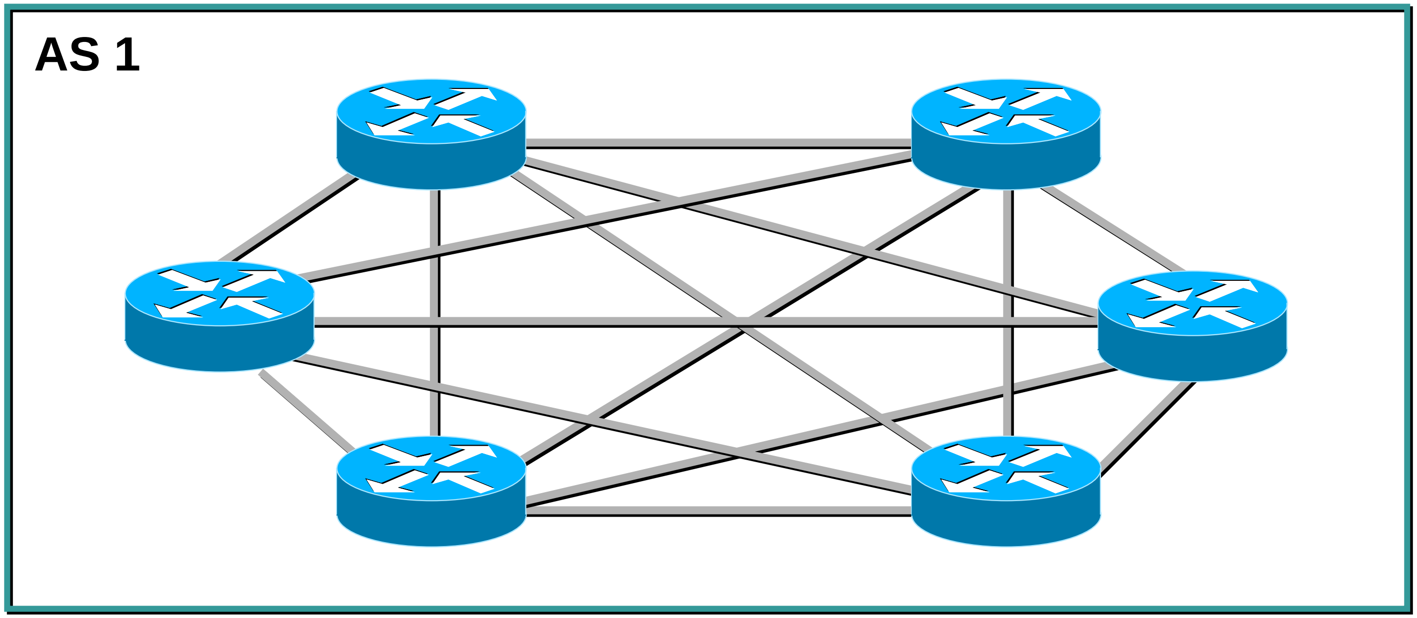
Route Maps

Route-map demo permit 10		
set	*as-path	Prepend String for a BGP AS-path Attribute
	automatic-tag	Automatically Compute TAG Value
	comm-list	Set BGP Community List (for Deletion)
	*community	BGP Community Attribute
	*dampening	Set BGP Route Flap Dampening Parameters
	default	Set Default Information
	interface	Output Interface
	*ip	IP Specific Information
	level	Where to Import Route
	*local-preference	BGP Local Preference Path Attribute
	*metric	Metric Value for Destination Routing Protocol
	metric-type	Type of Metric for Destination Routing Protocol
	*origin	BGP Origin Code
	tag	Tag Value for Destination Routing Protocol
	*weight	BGP Weight for Routing Table

Commands—Router

IBGP

- **IBGP requires a full mesh since IBGP speakers will not propagate routes learned from other IBGP speakers; the number of IBGP connections required is**
  - **[(N)(N-1)]/2 where N is the number of IBGP routers**
  - **For 6 routers, 15 logical IBGP connections are required**

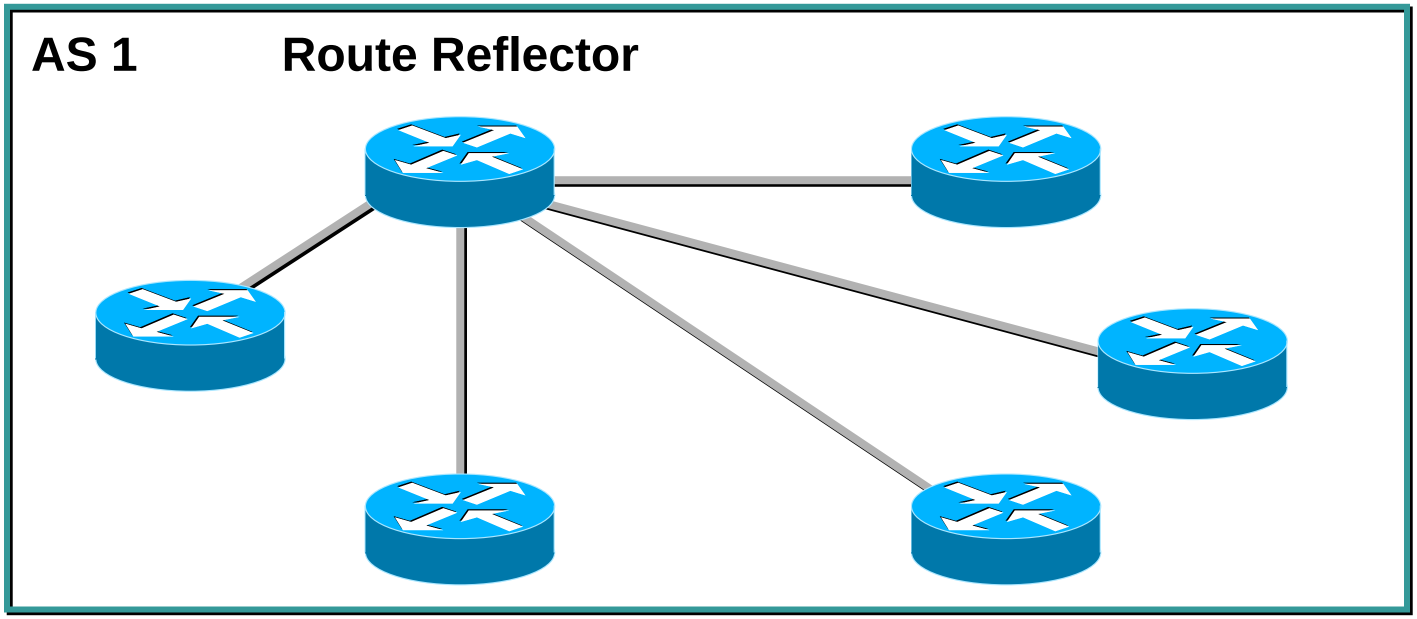


Commands—Router

Cisco.com

IBGP

Solution 1—Route Reflector

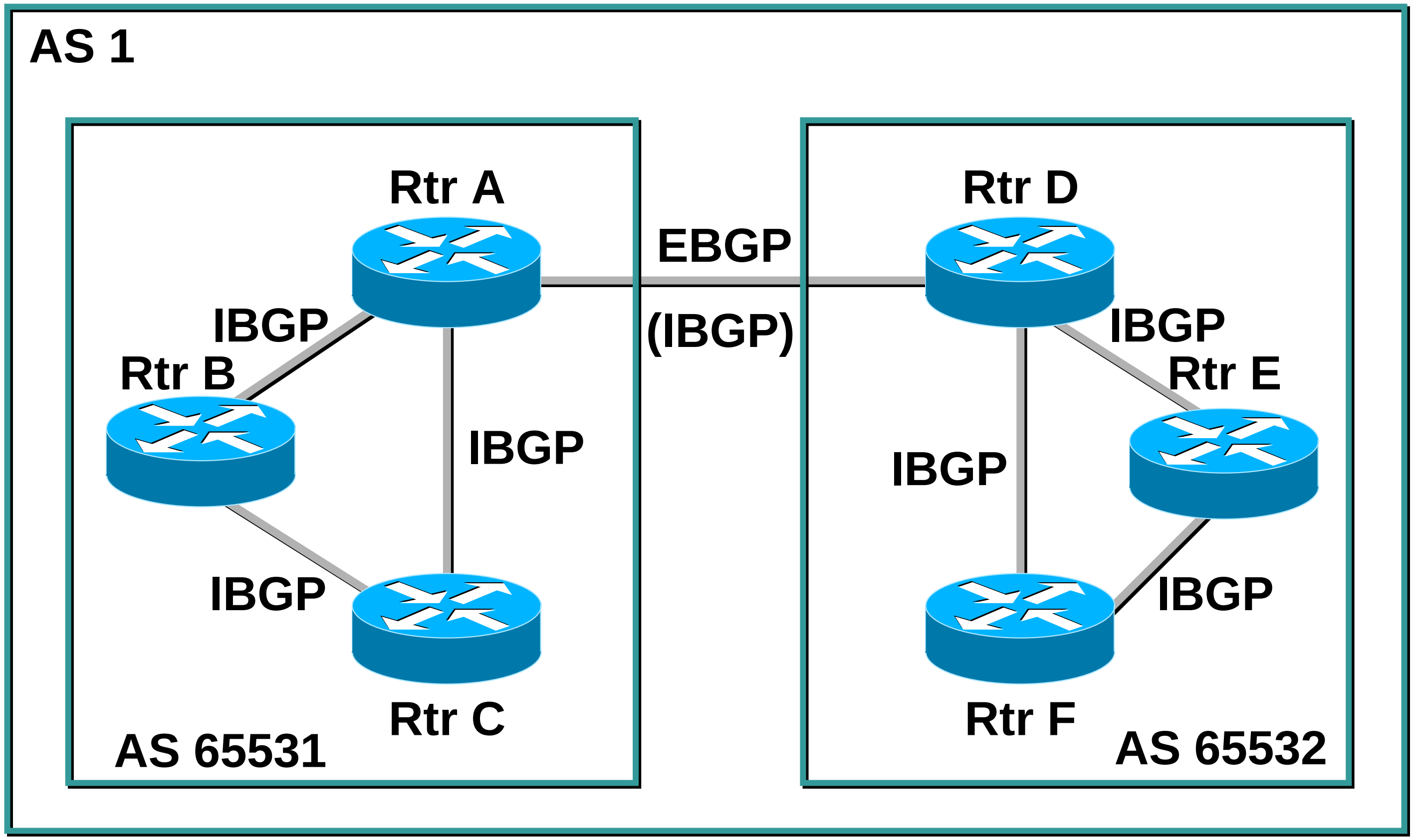


- **Only the route reflector needs additional configuration**
- **Neighbor x.x.x.x route-reflector-client**

Commands—Router

IBGP

Solution 2—Confederation



Commands—Router

IBGP

Confederation Configuration

Rtr A

```
router bgp 65531
 bgp confederation identifier 1
 bgp confederation peers 65532
 neighbor (Rtr B) remote-as 65531
 neighbor (Rtr C) remote-as 65531
 neighbor (Rtr D) remote-as 65532
```

Rtr D

```
router bgp 65532
 bgp confederation identifier 1
 bgp confederation peers 65531
 neighbor (Rtr A) remote-as 65531
 neighbor (Rtr E) remote-as 65532
 neighbor (Rtr F) remote-as 65532
```

Commands—Router

Neighbor

```
Rtr(config-router)#neighbor 1.1.1.1 ?
```

**advertise-map	Specify Route-Map for Conditional Advertisement
*advertisement-interval	Minimum Interval between Sending EBGP Routing Updates
**default-originate	Originate Default Route to this Neighbor
description	Neighbor Specific Description
***distribute-list	Filter Updates to/from this Neighbor
**ebgp-multihop	Allow EBGP Neighbors Not on Directly Connected Networks
**filter-list	Establish BGP Filters
*maximum-prefix	Maximum Number of Prefix Accept from this Peer
***next-hop-self	Disable the Next Hop Calculation for this Neighbor
*password	Set a Password
*peer-group	Member of the Peer-Group
*prefix-list	Filter Updates to/from this Neighbor

Importance: ***High **Medium *Low

Commands—Router

Neighbor

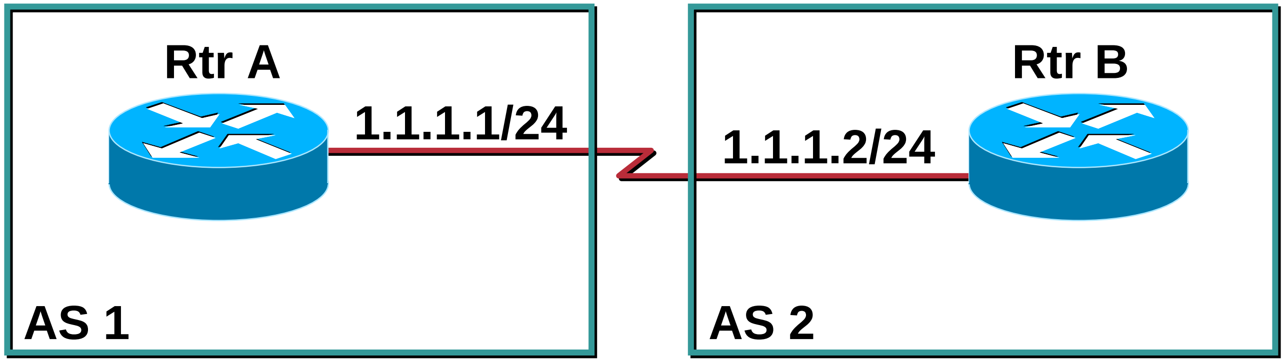
```
Rtr(config-router)#neighbor 1.1.1.1 ?
```

***remote-as	Specify a BGP Neighbor
*remove-private-AS	Remove Private AS Number from Outbound Updates
***route-map	Apply Route Map to Neighbor
***route-reflector-client	Configure a Neighbor as Route Reflector Client
**send-community	Send Community Attribute to this Neighbor
*shutdown	Administratively Shut Down this Neighbor
*soft-reconfiguration	Per Neighbor Soft Reconfiguration
*timers	BGP Per Neighbor Timers
**unsuppress-map	Route-Map to Selectively Unsuppress Suppressed Routes
**update-source	Source of Routing Updates
*version	Set the BGP Version to Match a Neighbor
**weight	Set Default Weight for Routes from this Neighbor

Importance: ***High **Medium *Low

Debugging

- Test the IP connection between the BGP Routers

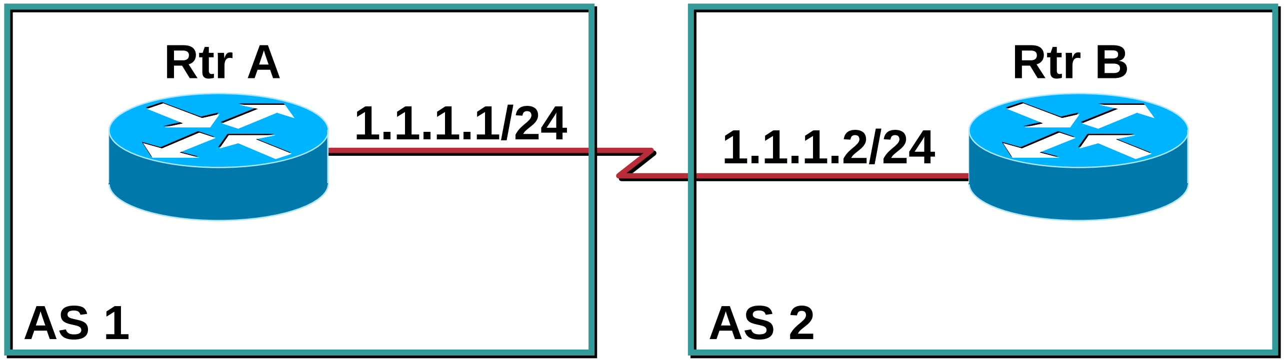


- If you can ping the remote endpoint then you can form a BGP connection

Rtr A#ping 1.1.1.2 **Rtr B#ping 1.1.1.1**

Debugging

- Start with a minimum BGP configuration



```
Rtr A#

router bgp 1
 neighbor 1.1.1.2 remote-as 2
```

```
Rtr B#

router bgp 2
 neighbor 1.1.1.1 remote-as 1
```

Check the BGP Connection

```
Rtr#show ip bgp ?
  A.B.C.D           IP Prefix <network>/<length>, e.g., 35.0.0.0/8
  A.B.C.D           Network in the BGP Routing Table to Display
  cidr-only         Display Only Routes with Non-Natural Netmasks
  community         Display Routes Matching the Communities
  community-list    Display Routes Matching the Community-list
  dampened-paths    Display Paths Suppressed Due to Dampening
  filter-list       Display Routes Conforming to the Filter-list
  flap-statistics   Display Flap Statistics of Routes
  inconsistent-as   Display Only Routes with Inconsistent Origin ASs
  neighbors         Detailed Information on TCP and BGP Neighbor Connections
  paths             Path Information
  peer-group        Display Information on Peer-Groups
  regexp            Display Routes Matching the AS Path Regular Expression
  summary           Summary of BGP Neighbor Status
  <cr>
```

Debugging

- **IF BGP state = Established then continue with your BGP configuration**

```
Rtr A#show ip bgp neighbors

BGP neighbor is 1.1.1.2,  remote AS 2, external link
  BGP version 4, remote router ID 1.1.1.2
  BGP state = Established, table version = 1, up for 0:12:20
  Last read 0:00:20, hold time is 180, keepalive interval is 60 seconds
  Minimum time between advertisement runs is 30 seconds
  Received 15 messages, 0 notifications, 0 in queue
  Sent 15 messages, 0 notifications, 0 in queue
  Connections established 1; dropped 0
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.1.1.7, Local port: 11002
Foreign host: 10.1.1.1, Foreign port: 179
```

References

- **Internet Routing Architectures, Bassam Halabi, Cisco Press**
- **Cisco BGP-4 Command and Configuration Handbook, William Parkhurst, Cisco Press**
- **BGP4 Case Studies/Tutorial Section 1-5**

  http://www.cisco.com/warp/public/459/13.html

  http://www.cisco.com/warp/public/459/14.html

  http://www.cisco.com/warp/public/459/15.html

  http://www.cisco.com/warp/public/459/16.html

  http://www.cisco.com/warp/public/459/17.html

References

- **Regular Expressions**

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios11/arbook/arapptrn.htm

Questions?

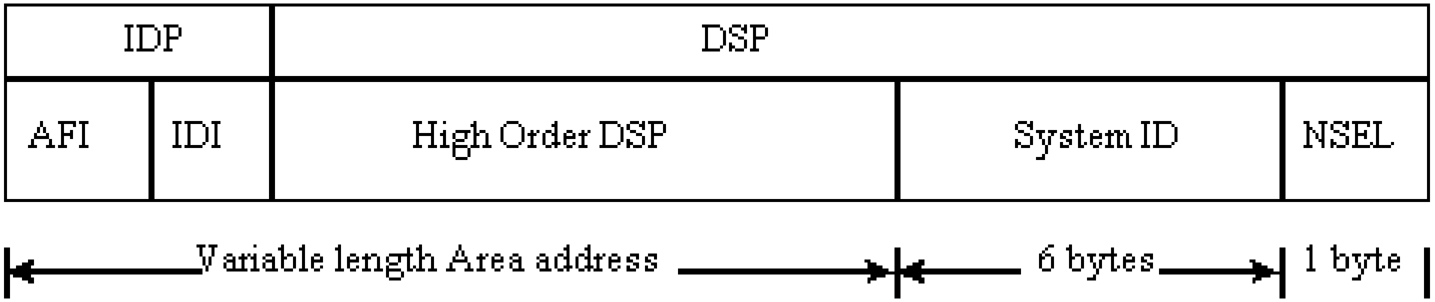
Cisco.com

ISIS

NSAPs and Addressing

- NSAP: Network Service Access Point
- An NSAP has an address that consists of 3 parts
  - Variable length area-address
  - 6 Byte system ID
  - 1 Byte n-selector (indicating transport layer)
- Total length between 8 and 20 bytes

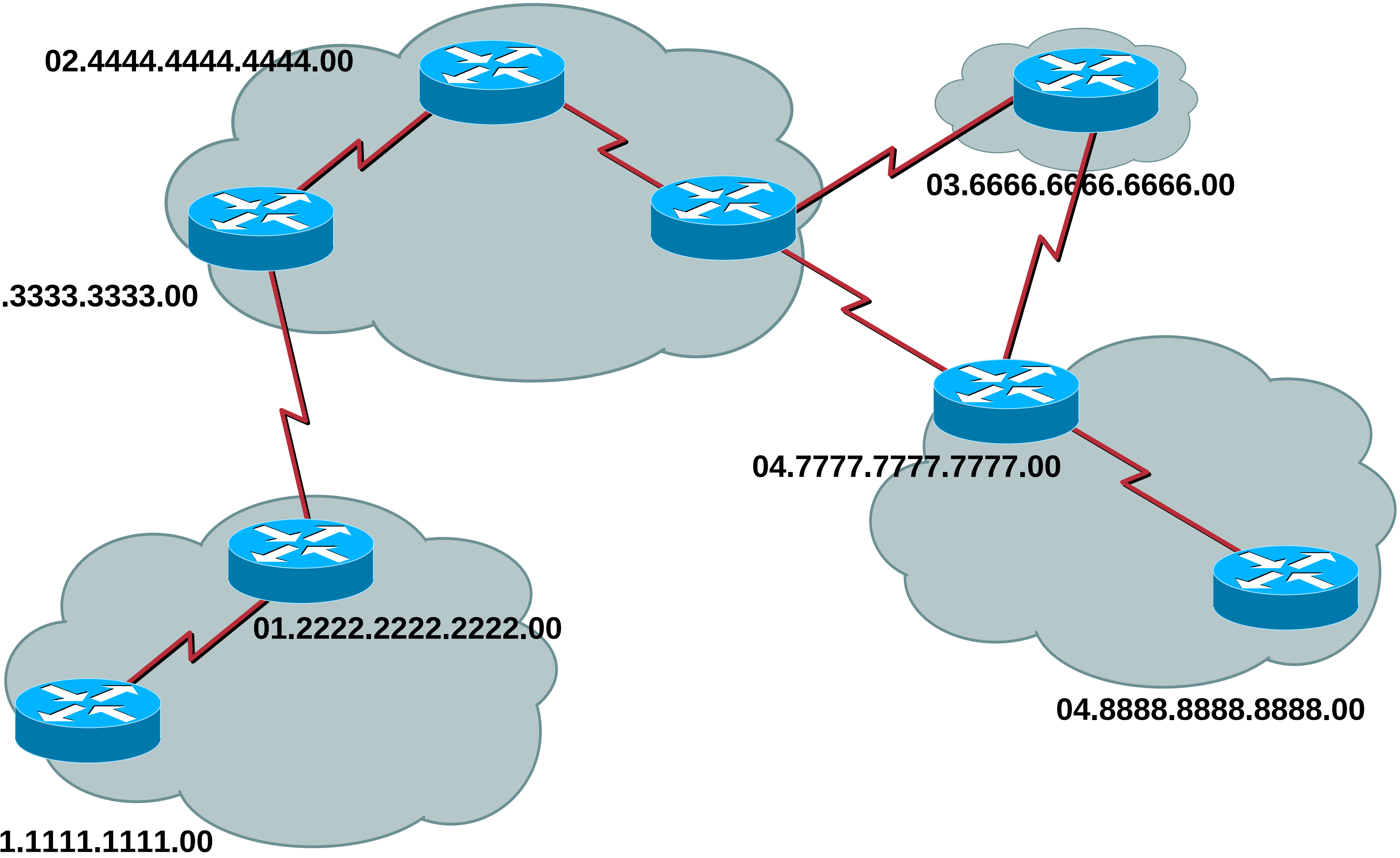
NSAPs and Addressing



- **ISO/IEC 10589 distinguishes only 3 fields in the NSAP address format**
  - **Area Address: variable length field composed of high order octets of the NSAP excluding the SystemID and SEL fields**
  - **SystemID: defines an ES or IS in an area; Cisco implements a fixed length of 6 octets for the SystemID**
  - **NSEL: selector, also designated as N-selector; it is the last byte of the NSAP and identifies a network service user (transport entity or the IS network entity itself)**

An Addressing Example

Cisco.com



Areas and Backbone Routers

- ISIS has a 2 layer hierarchy
  - The backbone (level-2)
  - The areas (level-1)
- An IS can be
  - Level-1 router (intra-area routing)
  - Level-2 router (inter-area routing)
  - Level-1-2 router (intra and inter-area routing)

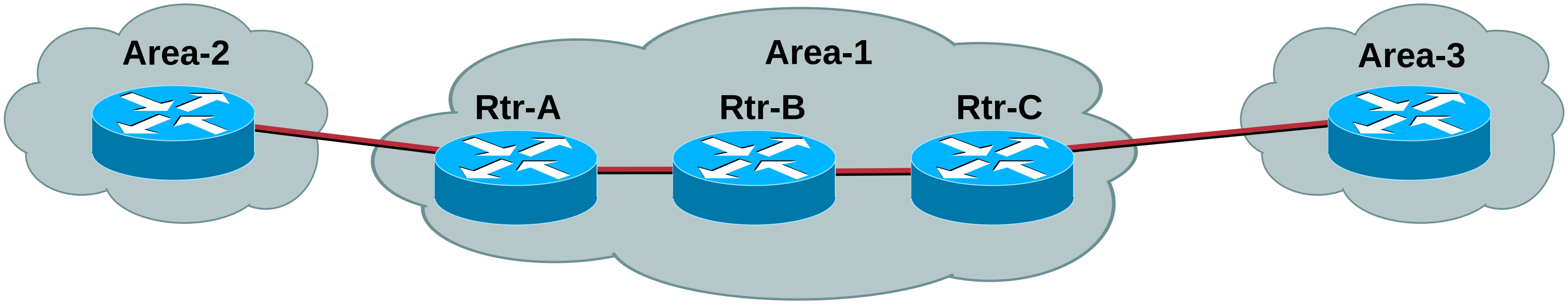
Areas and Backbone Routers

- ISIS does not have a backbone area
- The backbone is the contiguous collection of Level-2 capable routers
- More flexible and allows better scaling

The Backbone

- L2 routers must form contiguous backbone
    - L2 backbone is comparable with OSPF area 0
    - The backbone is the contiguous collection of L2 capable routers
- A router can’t tell whether it is a transit IS
    - Therefore the Cisco default is to be L1L2
    - Backbone will be larger then necessary
    - Always configure L1-only when possible
- Running L1L2 everywhere is less scalable
    - Especially with ISIS for IP

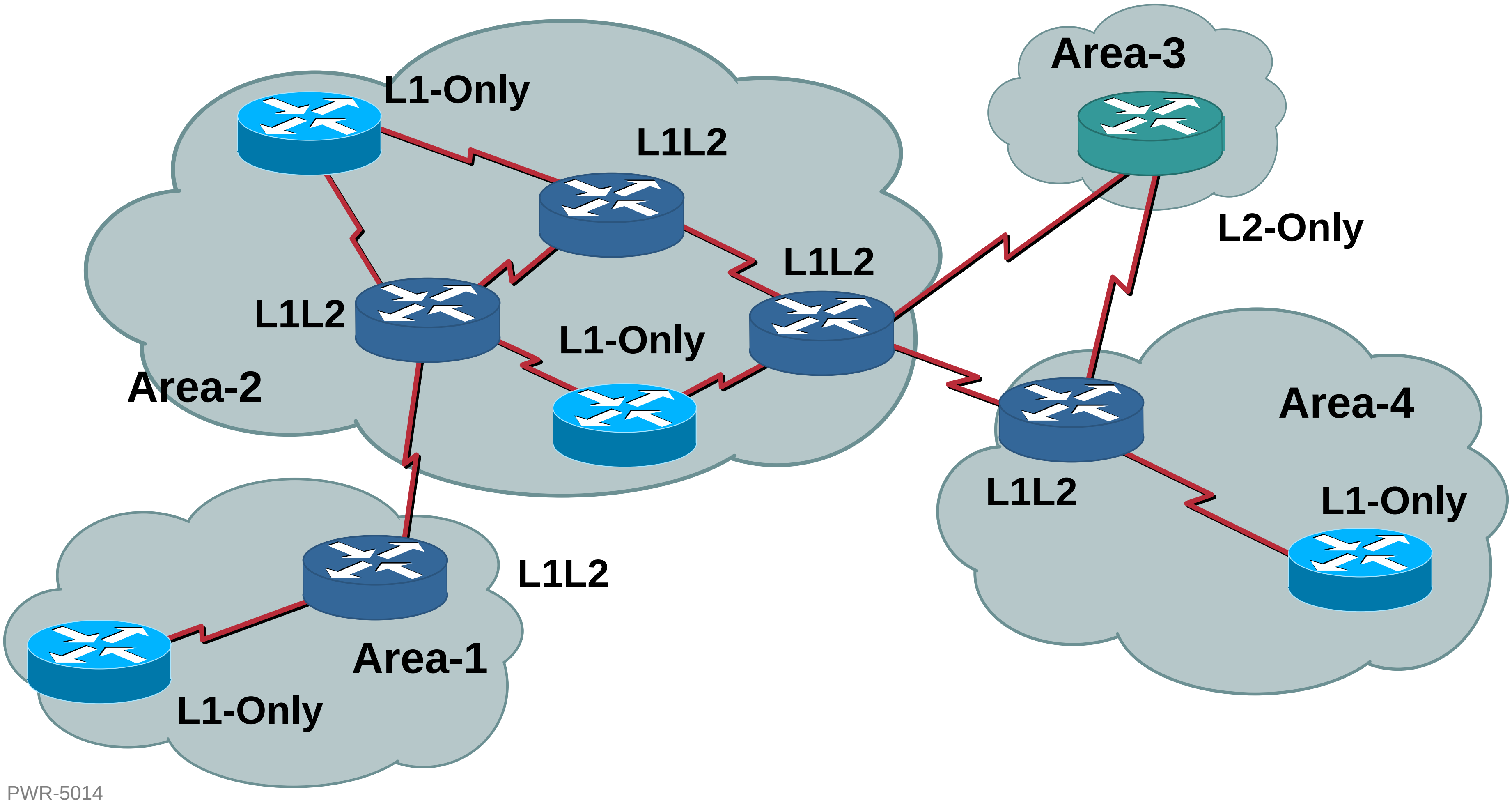
Level-1 vs. Level-2 Routing



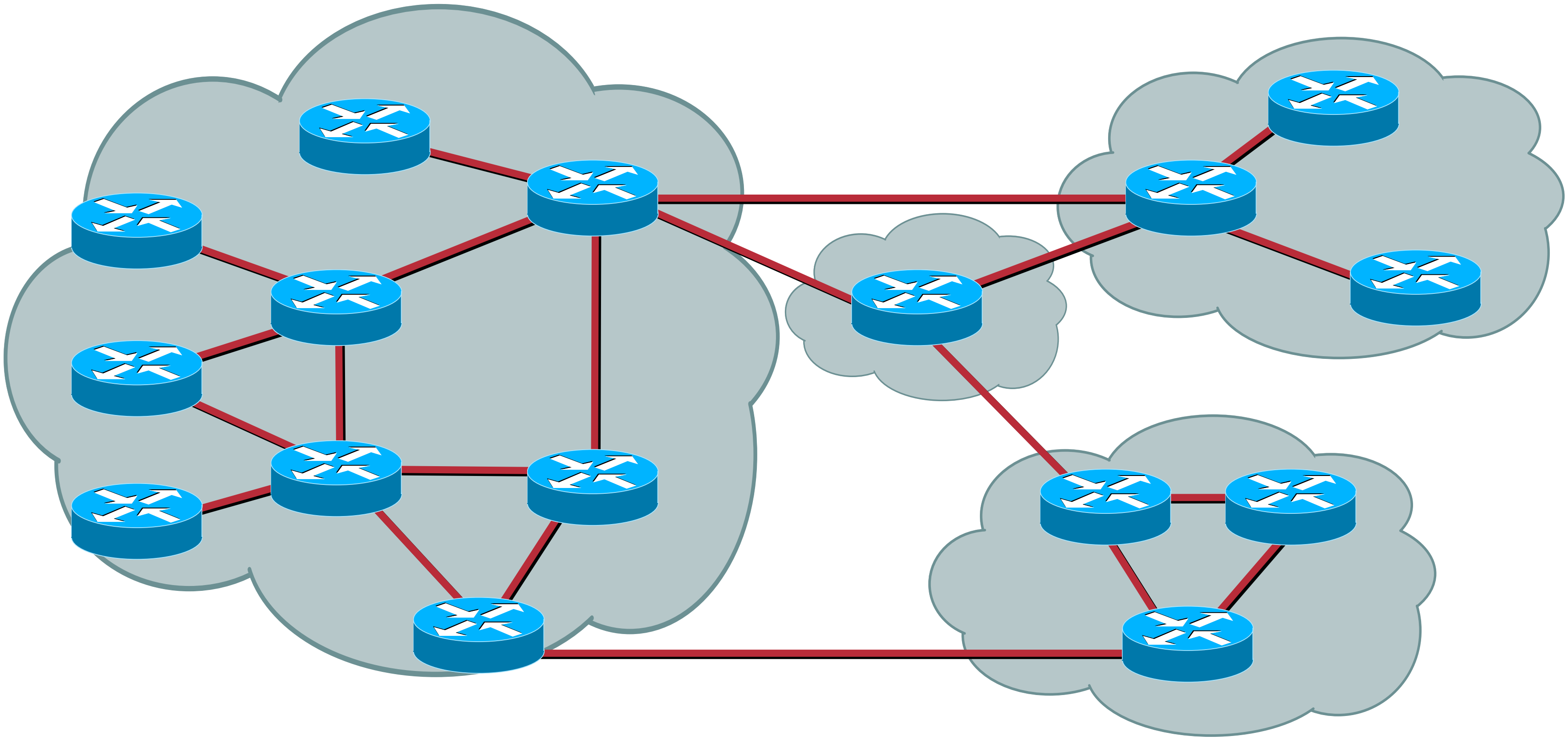
- Rtr-B has neighbors only in its own area
- Could have a level-1 behavior
- But Rtr-A and C rely on Rtr-B to connect areas 2 and 3
- Rtr-B must have a full L2 LSDB to route to areas 2 and 3
- The level-2 backbone must be contiguous
- So all Cisco routers try to be a L1L2 IS by default

L1, L2, and L1L2 Routers

- The backbone is the contiguous collection of L2 capable routers

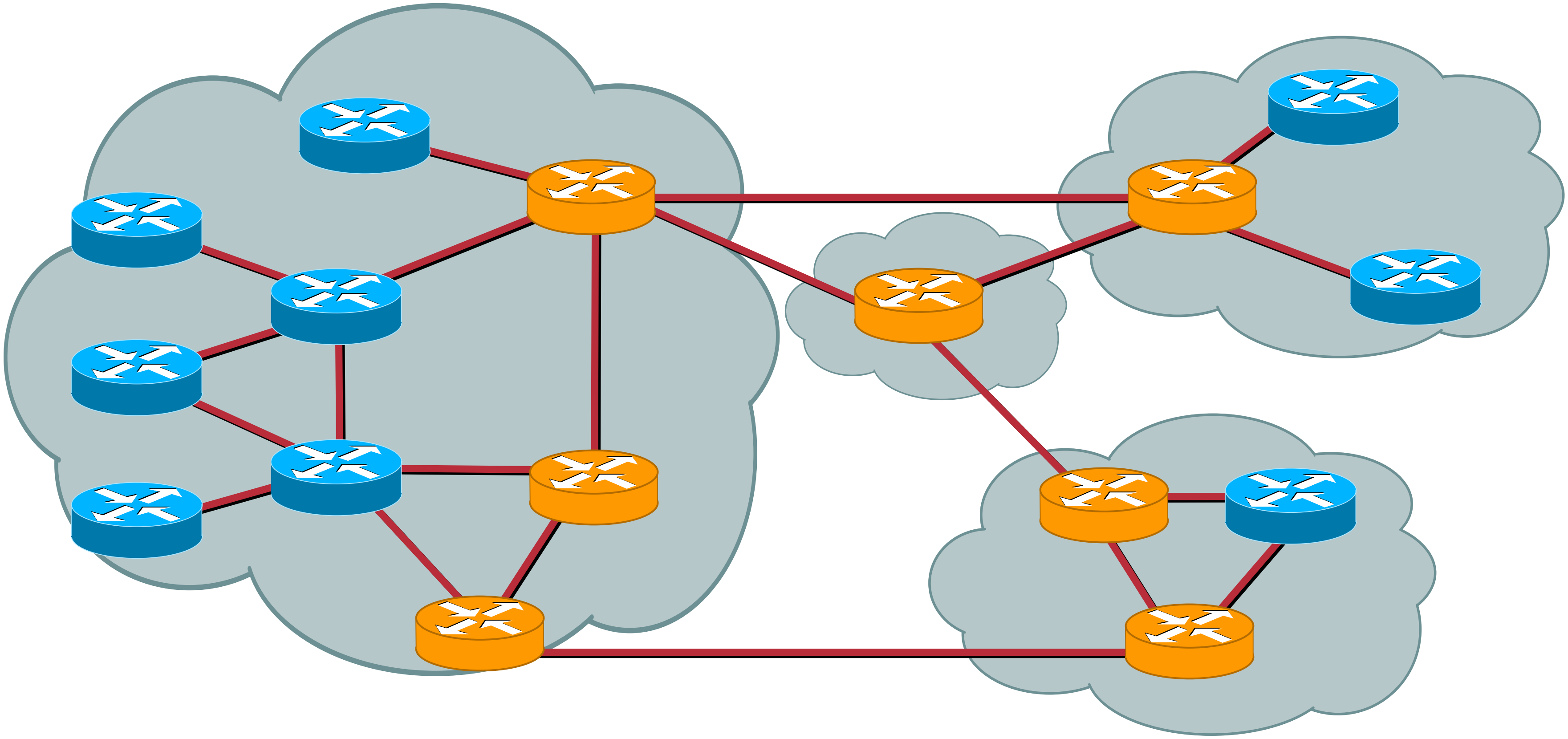


Configuring Level-1 and Level-2



- **What are the Level-2 capable routers?**

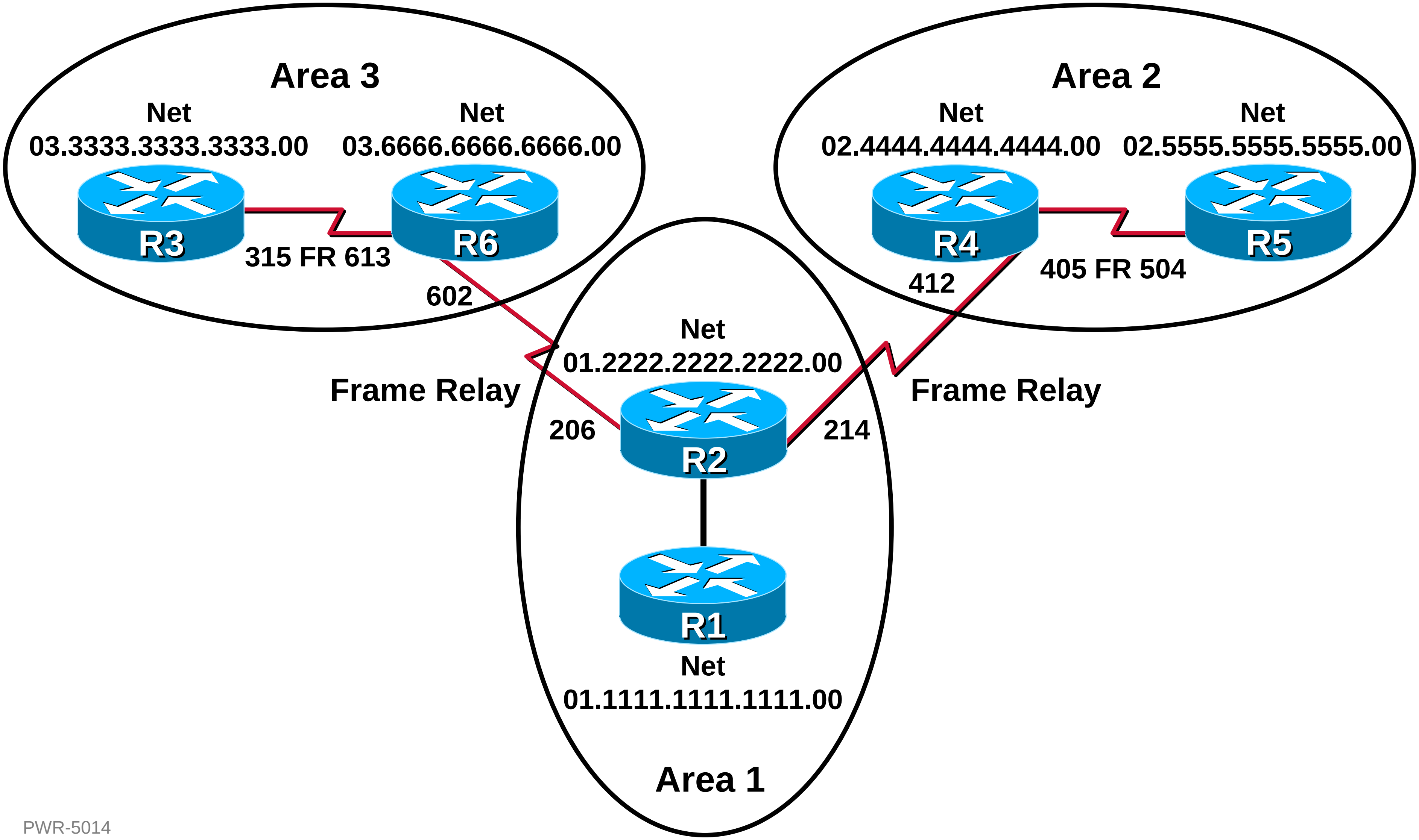
Configuring Level-1 and Level-2



- **What are the Level-2 capable routers?**

ISIS Configuration Example

Cisco.com



ISIS Configuration Example

R1

```
interface Loopback0
 ip address 10.1.11.11 255.255.255.0
 ip router isis
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
!
router isis
 net 01.1111.1111.1111.00
 is-type level-1
```

R3

```
interface Loopback0
 ip address 10.1.33.33 255.255.255.0
 ip router isis
!
interface Serial1
 ip address 10.1.4.3 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 316 broadcast
 frame-relay map ip 10.1.4.6 316 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
!
router isis
 net 03.3333.3333.3333.00
 is-type level-1
```

ISIS Configuration Example

Cisco.com

R2

```
interface Loopback0
 ip address 10.1.22.22 255.255.255.0
 ip router isis
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip router isis
!
interface Serial0/0
 ip address 10.1.3.2 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 206 broadcast
 frame-relay map ip 10.1.3.6 206 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
```

```
interface Serial0/1
 ip address 10.1.2.2 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 214 broadcast
 frame-relay map ip 10.1.2.4 214
broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
!
router isis
 net 01.2222.2222.2222.00
```

ISIS Configuration Example

R4

```
interface Loopback0
 ip address 10.1.44.44 255.255.255.0
 ip router isis
!
interface Serial0/0
 ip address 10.1.5.4 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 405 broadcast
 frame-relay map ip 10.1.5.5 405 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
```

```
interface Serial0/1
 ip address 10.1.2.4 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 412 broadcast
 frame-relay map ip 10.1.2.2 412 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
!
router isis
 net 02.4444.4444.4444.00
```

ISIS Configuration Example

R5

```
interface Loopback0
 ip address 10.1.55.55 255.255.255.0
 ip router isis
!
interface Serial0
 ip address 10.1.5.5 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 504 broadcast
 frame-relay map ip 10.1.5.4 504 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
!
router isis
 net 02.5555.5555.5555.00
 is-type level-1
```

ISIS Configuration Example

R6

```
interface Loopback0
 ip address 10.1.66.66 255.255.255.0
 ip router isis
!
interface Serial0/0
 ip address 10.1.3.6 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 602 broadcast
 frame-relay map ip 10.1.3.2 602 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
```

```
interface Serial0/1
 ip address 10.1.4.6 255.255.255.0
 ip router isis
 encapsulation frame-relay
 frame-relay map clns 613 broadcast
 frame-relay map ip 10.1.4.3 613 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
!
router isis
 net 03.6666.6666.6666.00
```

ISIS Configuration Example

```
R3#show clns neighbors

System Id     Interface   SNPA              State  Holdtime  Type
Protocol

Rack01R6       Se1       DLCI 316           Up     9          L1   IS-IS


R3#show isis topology

IS-IS paths to level-1 routers

System Id      Metric  Next-Hop       Interface       SNPA

Rack10R3        --

Rack01R6        10      R6              Se1             DLCI 316
```

References

- IS-IS Network Design Solutions, Abe Martey, Cisco Press
- Routing TCP/IP Volume 1, Jeff Doyle, Cisco Press
- Cisco Documentation

Cisco.com

Questions?

Session 6

Multicast/ATM/Security

Multicast

Multicast

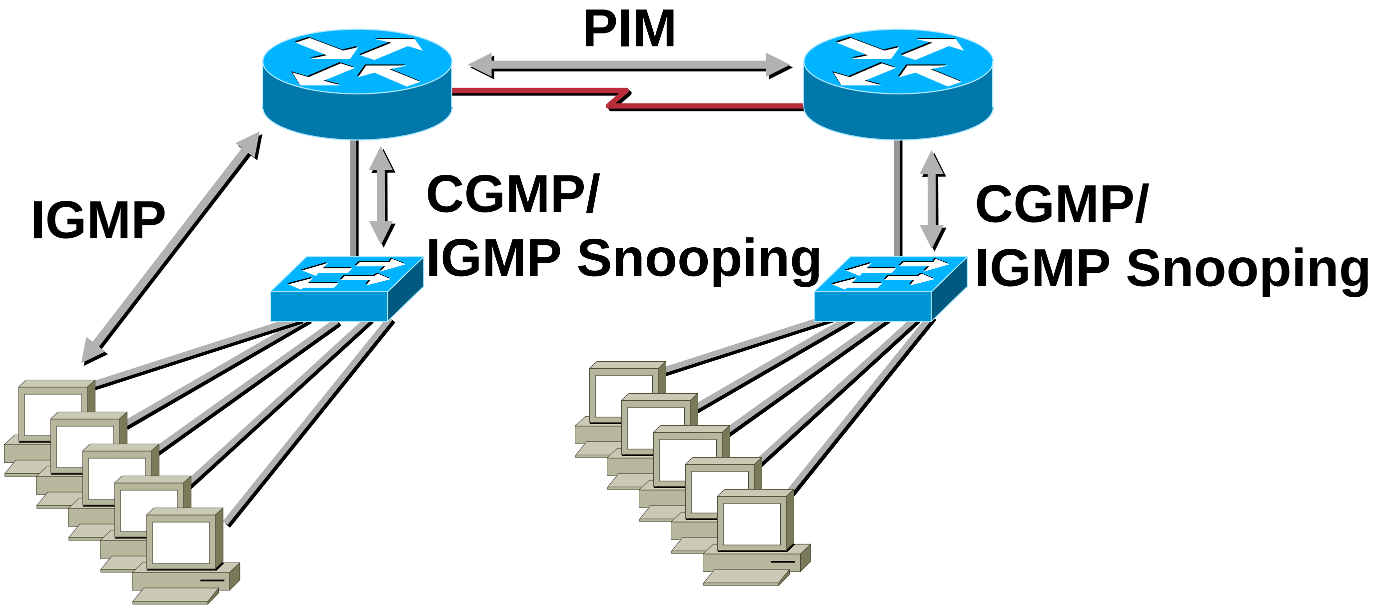
Cisco.com

- Overview
- Multicast Addressing and Forwarding
- PIM-DM Configuration and Verification
- PIM-SM Configuration and Verification
- References

Multicast

Cisco.com

Overview



PIM

IGMP

CGMP/
IGMP Snooping

CGMP/
IGMP Snooping

Multicast

Addressing

Class A	0.0.0.0 - 127.255.255.255
Class B	128.0.0.0 - 191.255.255.255
Class C	192.0.0.0 - 223.255.255.255
Class D	224.0.0.0 - 239.255.255.255

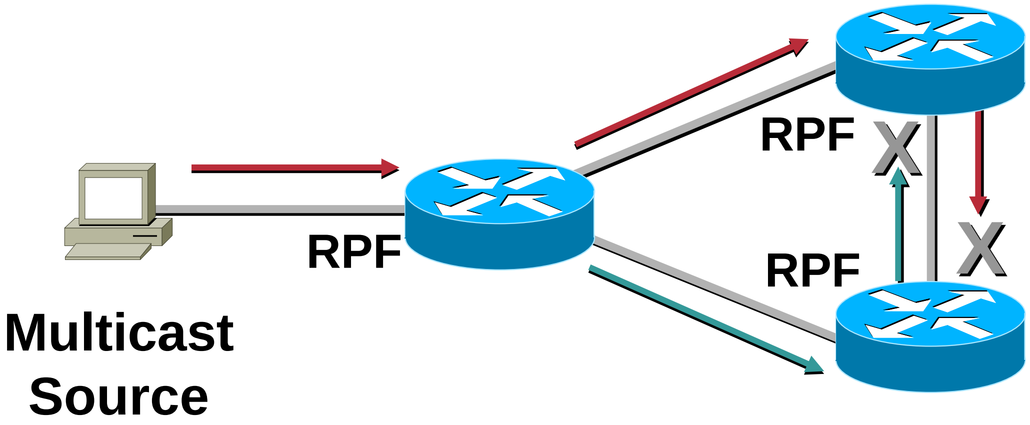
- Class A, B, and C IP packets are forwarded based on the destination address; Class D (multicast) packets are forwarded based on the source IP address

Multicast

Cisco.com

Loop Detection

- A multicast packet received on an interface will be accepted if received on the interface that would be used to send a unicast IP packet back to the source; this is called Reverse Path Forwarding (RPF)

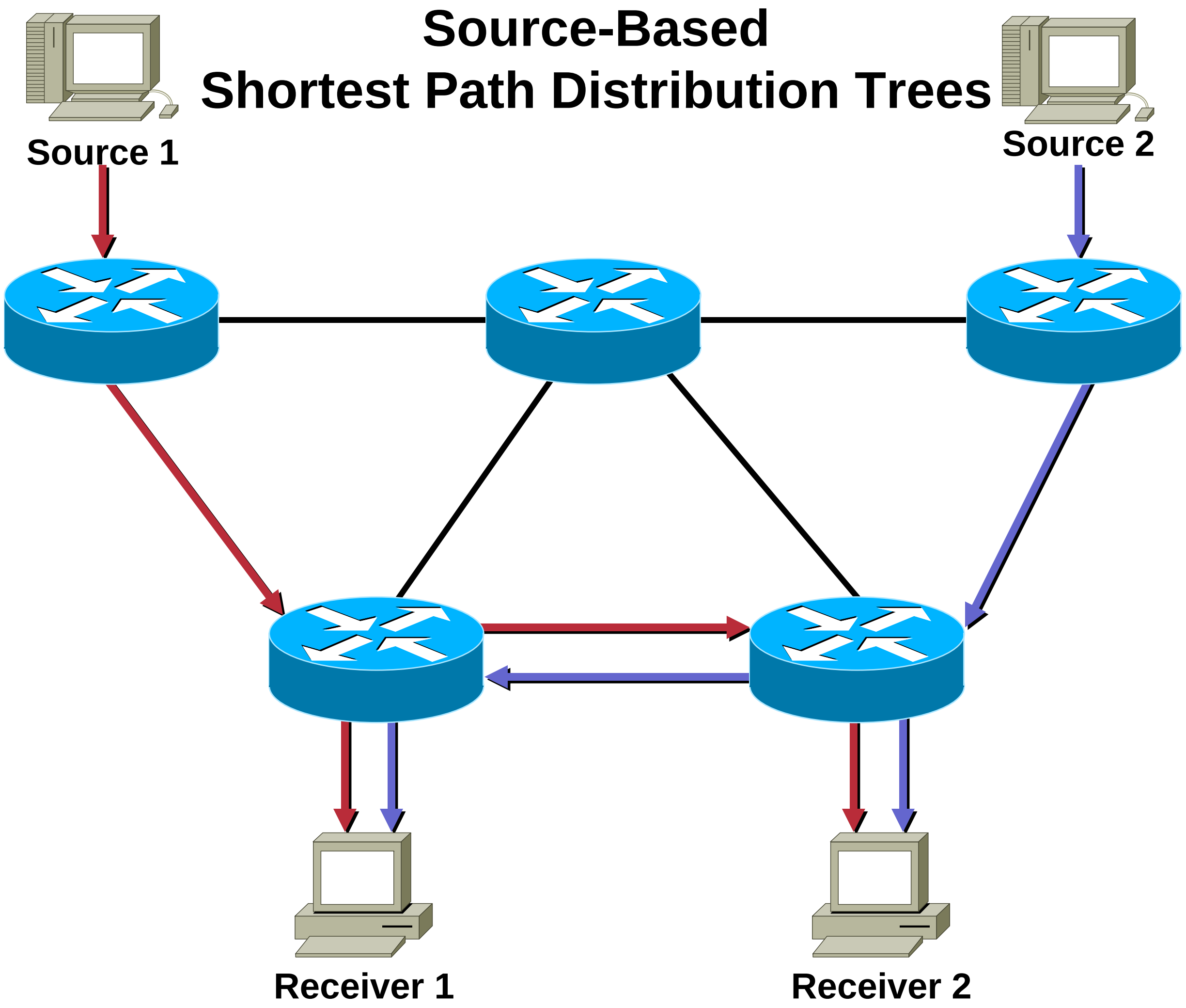


Multicast—Dense Mode

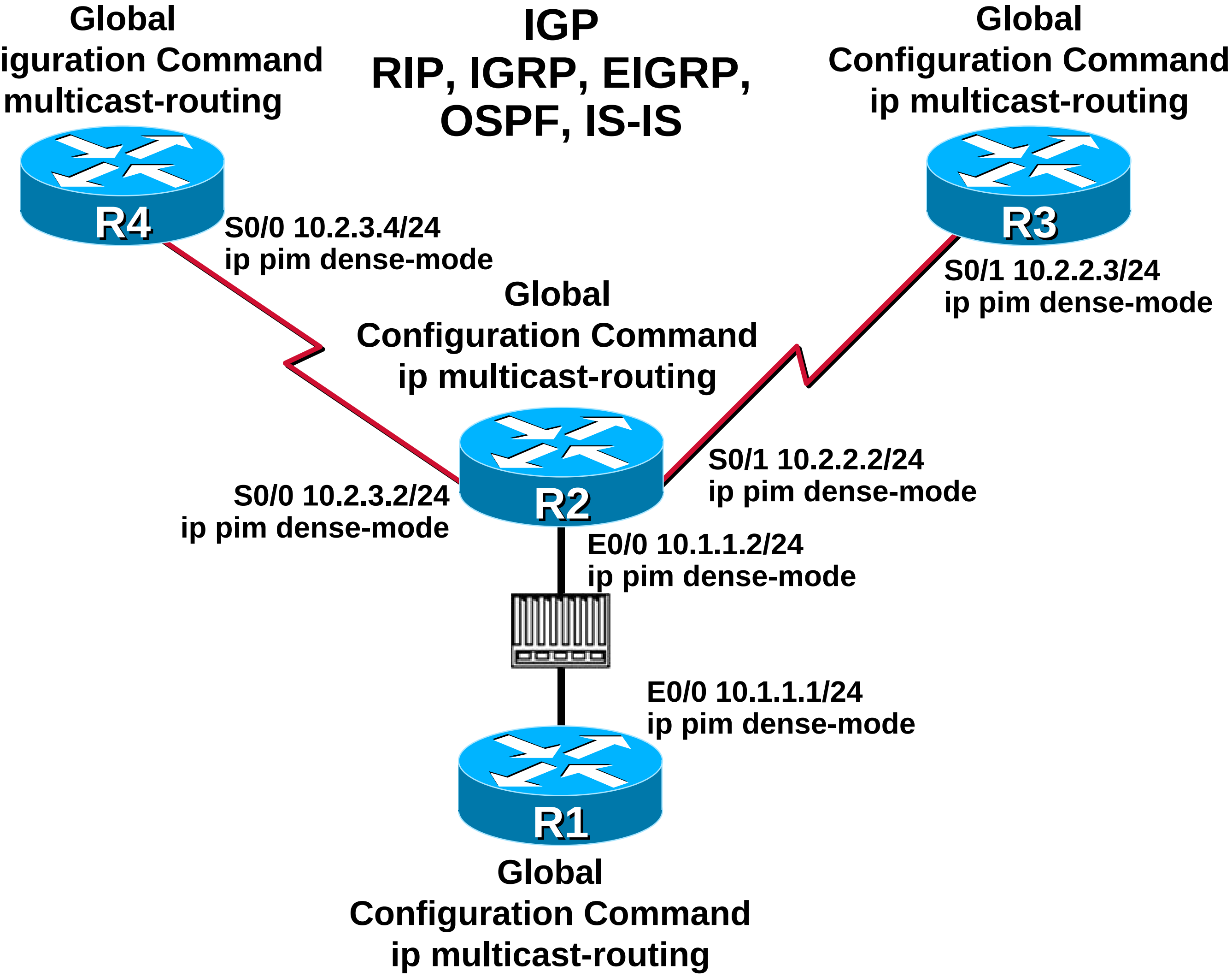
- Protocol-independent
  - Supports all underlying unicast routing protocols including: static, RIP, IGRP, EIGRP, IS-IS, BGP, and OSPF
- Dense-mode
  - Uses “Push” Model
  - Traffic flooded throughout network
  - Pruned back where it is unwanted
  - Flood and Prune behavior (typically every 3 minutes)

Multicast—Dense Mode

Cisco.com



Multicast—Dense Mode Configuration



IGP
RIP, IGRP, EIGRP, OSPF, IS-IS

R4
Global Configuration Command
ip multicast-routing

S0/0 10.2.3.4/24
ip pim dense-mode

R3
Global Configuration Command
ip multicast-routing

S0/1 10.2.2.3/24
ip pim dense-mode

R2
Global Configuration Command
ip multicast-routing

S0/0 10.2.3.2/24
ip pim dense-mode

S0/1 10.2.2.2/24
ip pim dense-mode

E0/0 10.1.1.2/24
ip pim dense-mode

R1
E0/0 10.1.1.1/24
ip pim dense-mode

Global Configuration Command
ip multicast-routing

Multicast—Dense Mode Verification

```
r2#show ip pim interface

Address       Interface      Ver/   Nbr     Query   DR      DR
                             Mode   Count   Intvl   Prior
10.1.1.2      Ethernet0/0    v2/D   1       30      1       10.1.1.2
10.1.3.2      Serial0/0      v2/D   1       30      1       10.1.3.6
10.1.2.2      Serial0/1      v2/D   1       30      1       10.1.2.4
```

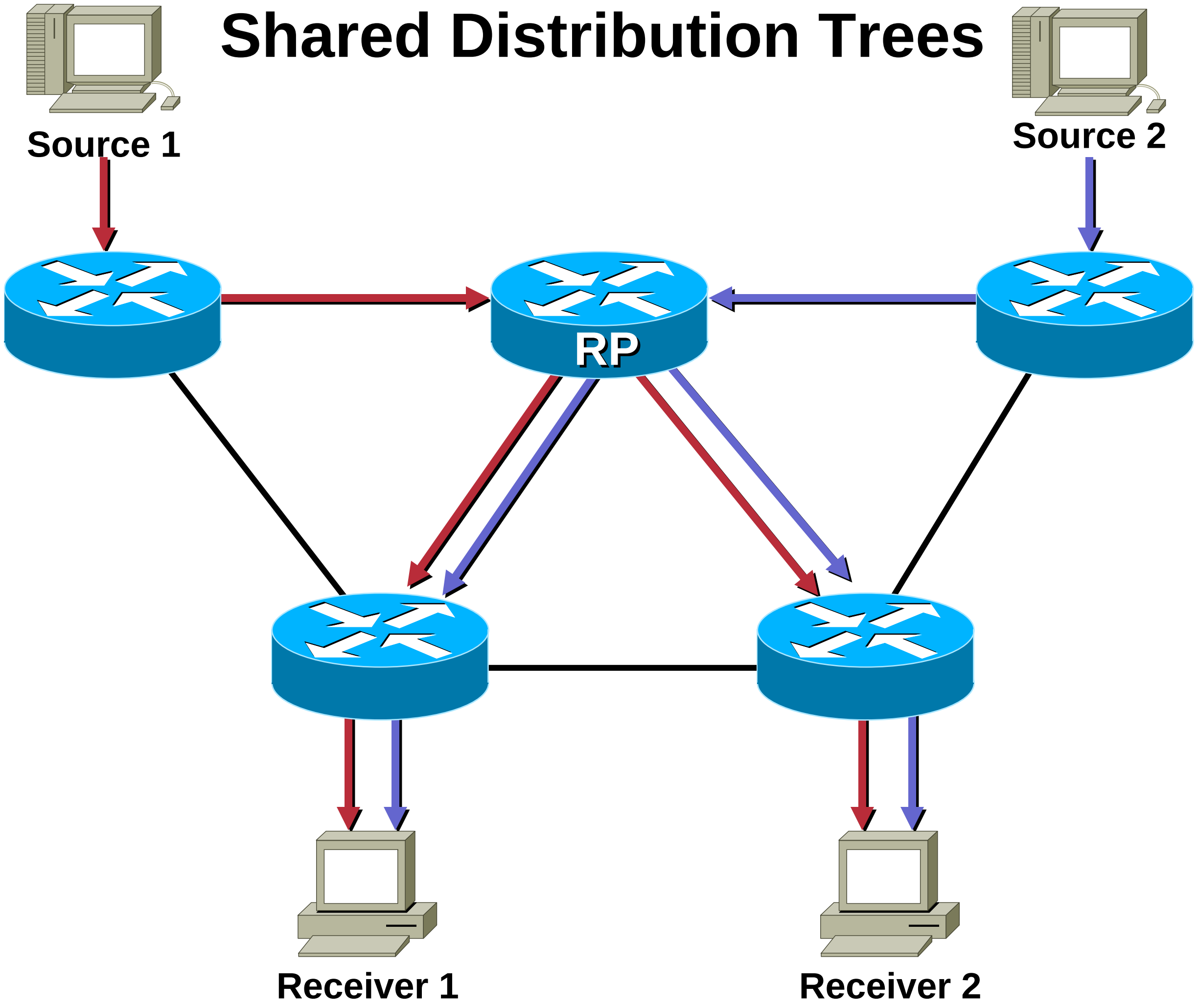
```
r2#show ip pim neighbor
PIM Neighbor Table
Neighbor      Interface      Uptime/Expires     Ver   DR
Address                                               Priority/Mode
10.1.1.1      Ethernet0/0    22:29:27/00:01:32 v2     1 / B S
10.1.3.6      Serial0/0      22:29:02/00:01:40 v2     1 / DR B S
10.1.2.4      Serial0/1      22:28:23/00:01:41 v2     1 / DR B S
```

Multicast—Sparse Mode

- Protocol-independent
  - Supports all underlying unicast routing protocols including: static, RIP, IGRP, EIGRP, IS-IS, BGP, and OSPF
- Sparse-mode
  - Uses “Pull” model
  - Traffic sent only to where it is requested
  - Explicit join behavior

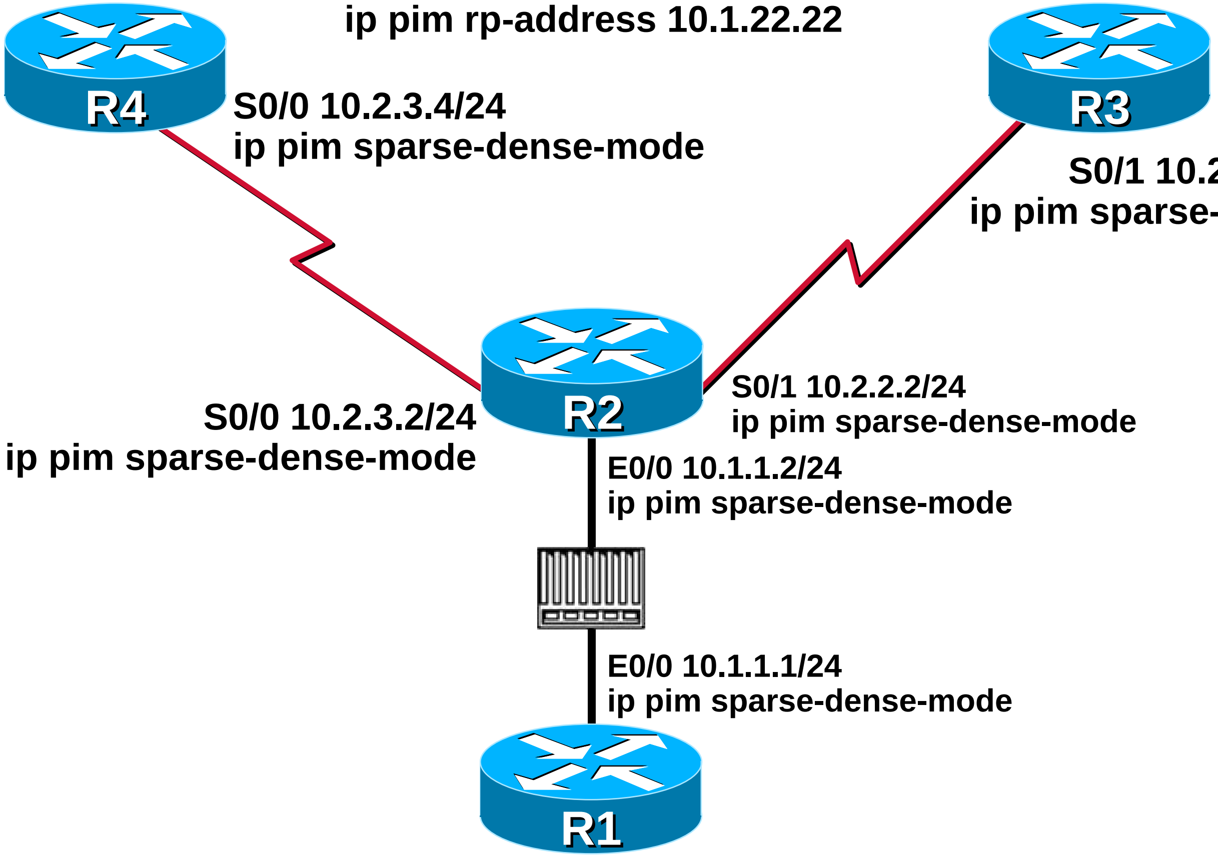
Multicast—Sparse Mode

Shared Distribution Trees



Multicast—Sparse Mode Static RP

Cisco.com



On Every Router
Global Configuration Command

```
ip multicast-routing
ip pim rp-address 10.1.22.22
```

R4
S0/0 10.2.3.4/24
ip pim sparse-dense-mode

R3
S0/1 10.2.2.3/24
ip pim sparse-dense-mode

R2
S0/0 10.2.3.2/24
ip pim sparse-dense-mode

S0/1 10.2.2.2/24
ip pim sparse-dense-mode

E0/0 10.1.1.2/24
ip pim sparse-dense-mode

R1
E0/0 10.1.1.1/24
ip pim sparse-dense-mode

Multicast—Sparse Mode Static RP—Verification

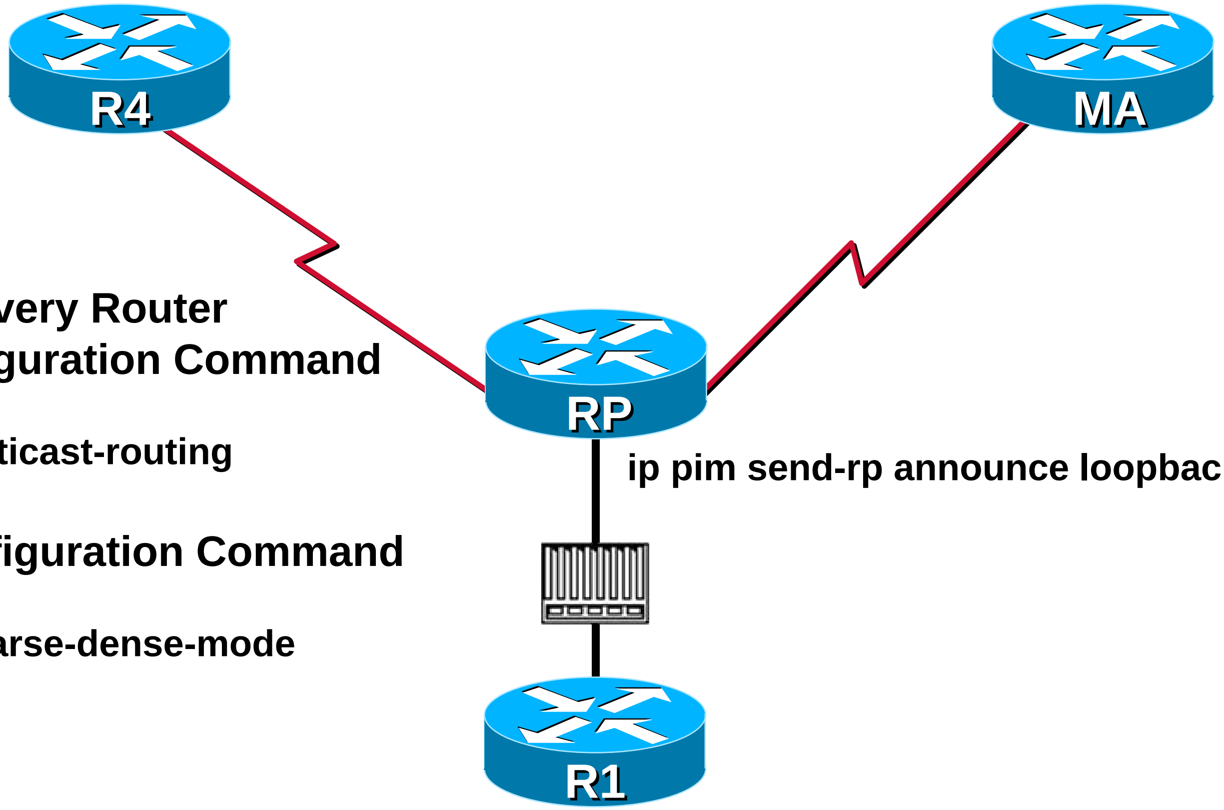
```
r3#show ip pim rp
Group: 224.0.1.40, RP: 10.1.22.22, v1, uptime 00:12:24, expires never

r2#show ip pim interface

Address          Interface          Ver/   Nbr      Query  DR     DR
                                    Mode Count  Intvl  Prior
10.1.1.2        Ethernet0/0       v2/SD  1          30        1        10.1.1.2
10.1.3.2        Serial0/0          v2/SD  1          30        1        10.1.3.6
10.1.2.2        Serial0/1          v2/SD  1          30        1        10.1.2.4

r2#show ip pim neighbor
PIM Neighbor Table
Neighbor        Interface           Uptime/Expires    Ver   DR
Address                                                       Priority/Mode
10.1.1.1         Ethernet0/0      1d00h/00:01:17    v2    1 / B S
10.1.3.6         Serial0/0          1d00h/00:01:44    v2    1 / DR B S
10.1.2.4         Serial0/1          1d00h/00:01:44    v2    1 / DR B S
```

Multicast—Sparse Mode Auto-RP

- Routers automatically learn RP address
  - Only routers that are candidate RPs or mapping agents need to be configured
- Makes use of Multicast to distribute info
  - Two specially IANA-assigned groups used
    - Cisco-Announce—224.0.1.39
    - Cisco-Discovery—224.0.1.40
  - Typically dense mode is used forward these groups
- Permits backup RP's to be configured

Multicast—Sparse Mode Auto-RP

Cisco.com



ip pim send-rp announce loopback 0 scope 16

On Every Router
Global Configuration Command

ip multicast-routing

Interface Configuration Command

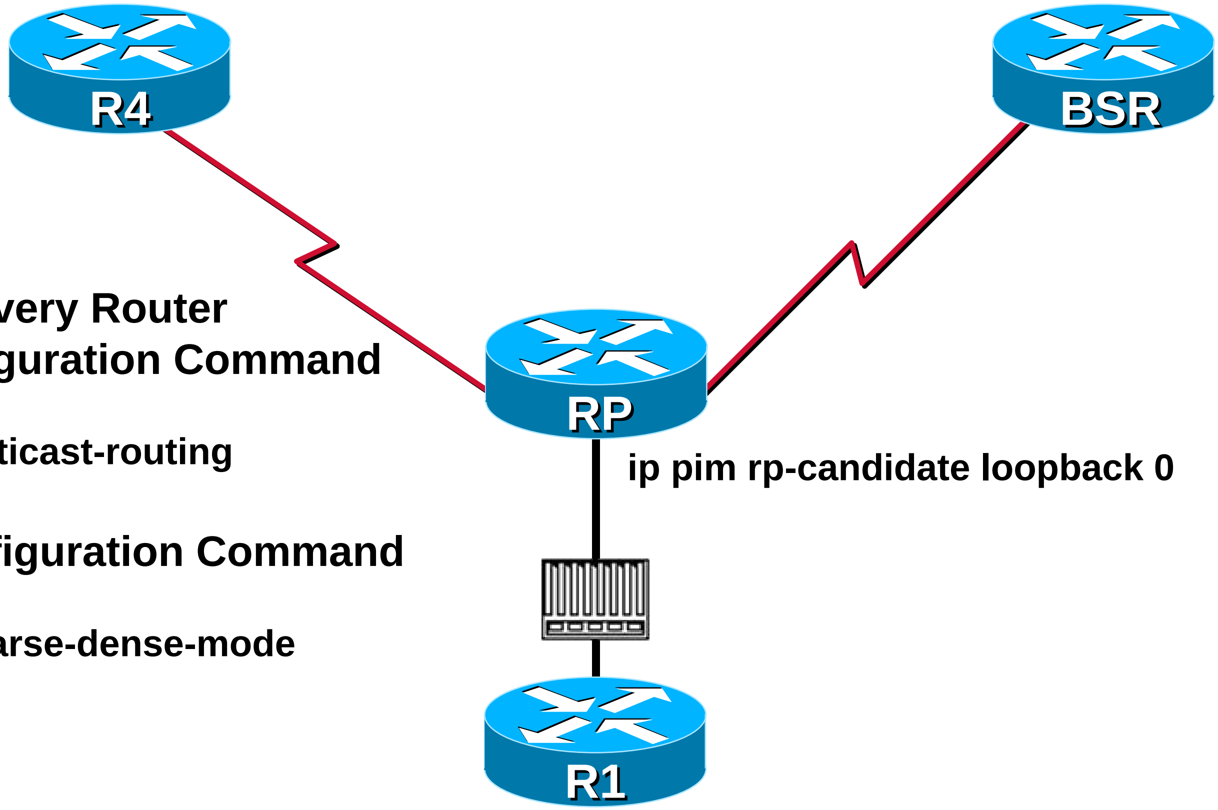
ip pim sparse-dense-mode

ip pim send-rp announce loopback 0 scope 16

Multicast—Sparse Mode Auto-RP Verification

```
r2#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)

Group(s) 224.0.0.0/4
  RP 10.1.22.22 (r2), v2v1
    Info source: 10.1.44.44 (?), via Auto-RP
         Uptime: 00:02:19, expires: 00:02:38

r3#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent (Loopback0)

Group(s) 224.0.0.0/4
  RP 10.1.22.22 (r2), v2v1
    Info source: 10.1.22.22 (?), via Auto-RP
         Uptime: 00:02:55, expires: 00:02:00

r4#show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 10.1.22.22 (r2), v2v1
    Info source: 10.1.44.44 (?), via Auto-RP
         Uptime: 00:24:29, expires: 00:02:17
```

Multicast—Sparse Mode BSR



ip pim bsr-candidate loopback 0

On Every Router
Global Configuration Command

ip multicast-routing

Interface Configuration Command

ip pim sparse-dense-mode

ip pim rp-candidate loopback 0

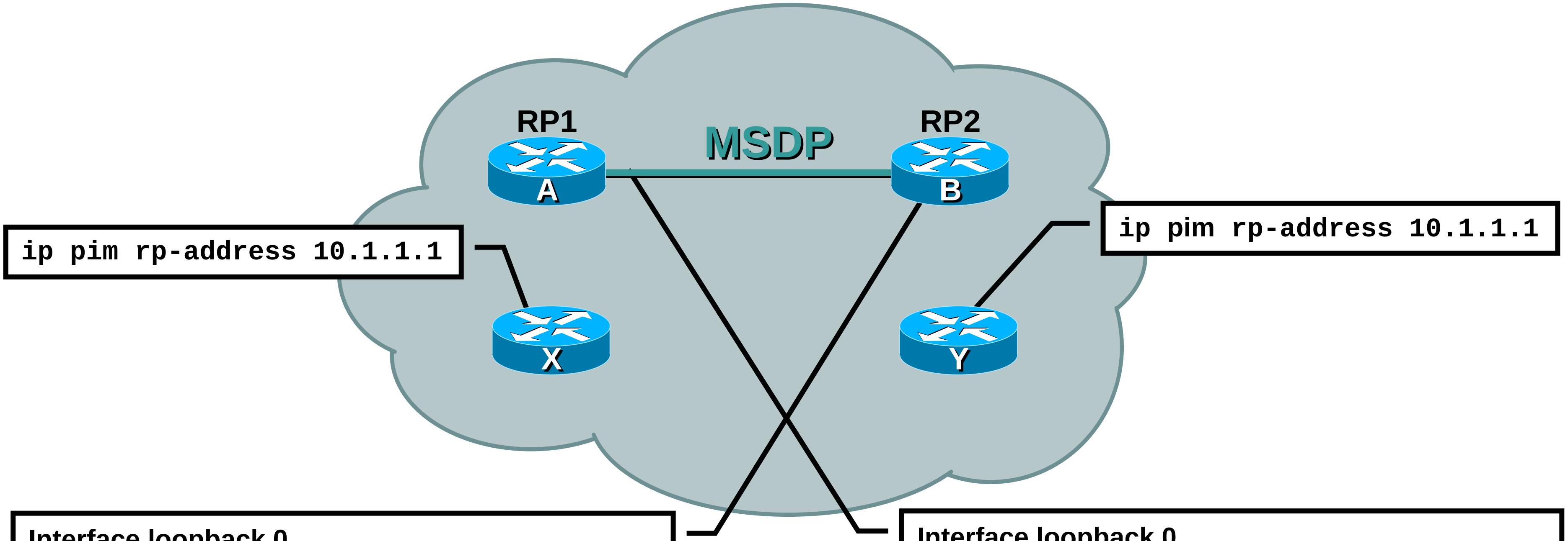
Multicast—Sparse Mode BSR Verification

```
r2#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)

Group(s) 224.0.0.0/4
  RP 10.1.22.22 (?), v2
    Info source: 10.1.44.44 (?), via bootstrap
         Uptime: 00:04:09, expires: 00:02:27

r2#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 10.1.44.44 (?)
  Uptime:      00:06:16, BSR Priority: 0, Hash mask length: 0
  Expires:     00:01:55

Next Cand_RP_advertisement in 00:00:39
  RP: 10.1.22.22(Loopback0)
```

Anycast RP—Overview

- Uses single statically defined RP address
  - Two or more routers have same RP address
    - RP address defined as a loopback interface
    - Loopback address advertised as a host route
  - Senders and receivers join/register with closest RP
    - Closest RP determined from the unicast routing table
  - Can never fall back to dense mode
    - Because RP is statically defined
- MSDP session(s) run between all RPs
  - Informs RPs of sources in other parts of network
  - RPs join SPT to active sources as necessary

Anycast RP Configuration



```
ip pim rp-address 10.1.1.1
```

```
ip pim rp-address 10.1.1.1
```

```
Interface loopback 0
  ip address 10.1.1.1 255.255.255.255

Interface loopback 1
 ip address 10.0.0.2 255.255.255.255
!
ip msdp peer 10.0.0.1 connect-source loopback 1
ip msdp originator-id loopback 1
```

```
Interface loopback 0
 ip address 10.1.1.1 255.255.255.255

Interface loopback 1
 ip address 10.0.0.1 255.255.255.255
!
ip msdp peer 10.0.0.2 connect-source loopback 1
ip msdp originator-id loopback 1
```

Preparation

- **References**

  Developing IP Multicast Networks; Beau Williamson, Cisco Press

  Routing TCP/IP Volume II; Jeff Doyle, Cisco Press

  ftp://ftpeng.cisco.com/ipmulticast/training/index.html

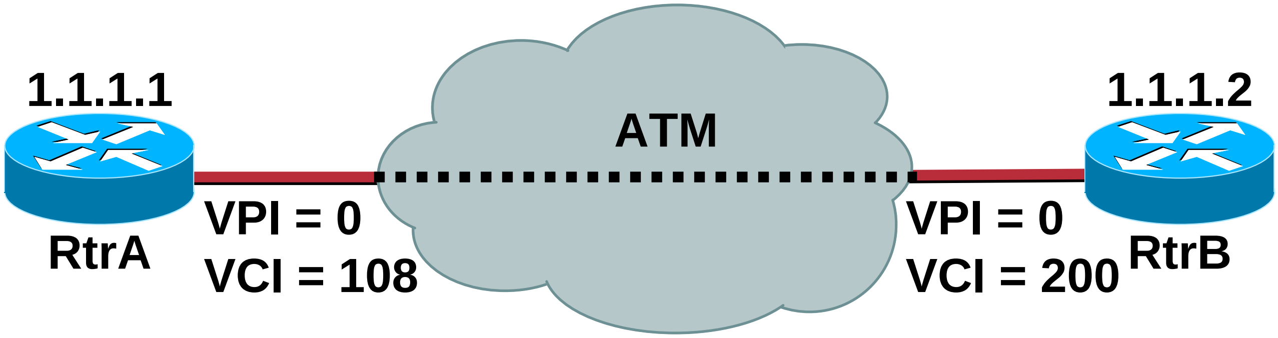
Questions?

ATM

ATM Topics

- Basic ATM Scenarios
  - PVC-Based
  - Classical IP-over-ATM
- ATM Feature Example

PVC Scenario



1.1.1.1

RtrA

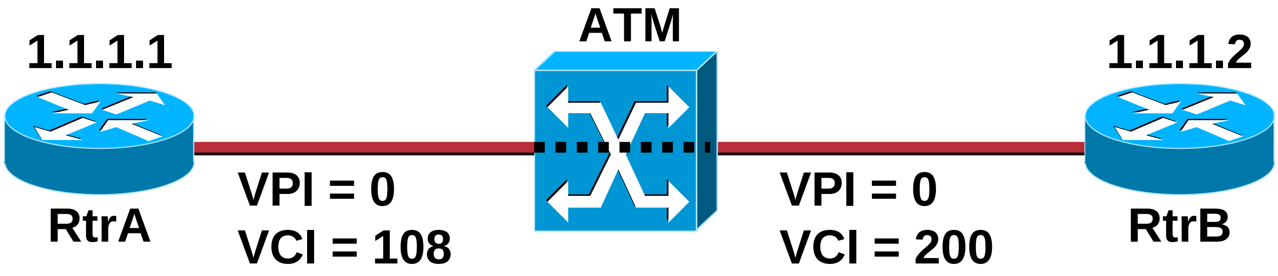
VPI = 0
VCI = 108

ATM

1.1.1.2

VPI = 0
VCI = 200

RtrB



1.1.1.1

RtrA

VPI = 0
VCI = 108

ATM

1.1.1.2

VPI = 0
VCI = 200

RtrB

PVC Scenario (Cont.)

End-Station Configuration Example

```
hostname RtrA
!
interface ATM3/0
 no ip address
!
interface ATM3/0.1 point-to-multipoint
 ip address 1.1.1.1 255.255.255.0
 pvc 0/108
  protocol ip 1.1.1.2
  broadcast
  encapsulation aal5snap
```

IP Address
for this Side of PVC

Define VPI/VCI Values for PVC

IP Address for Remote Host

PVC Attributes

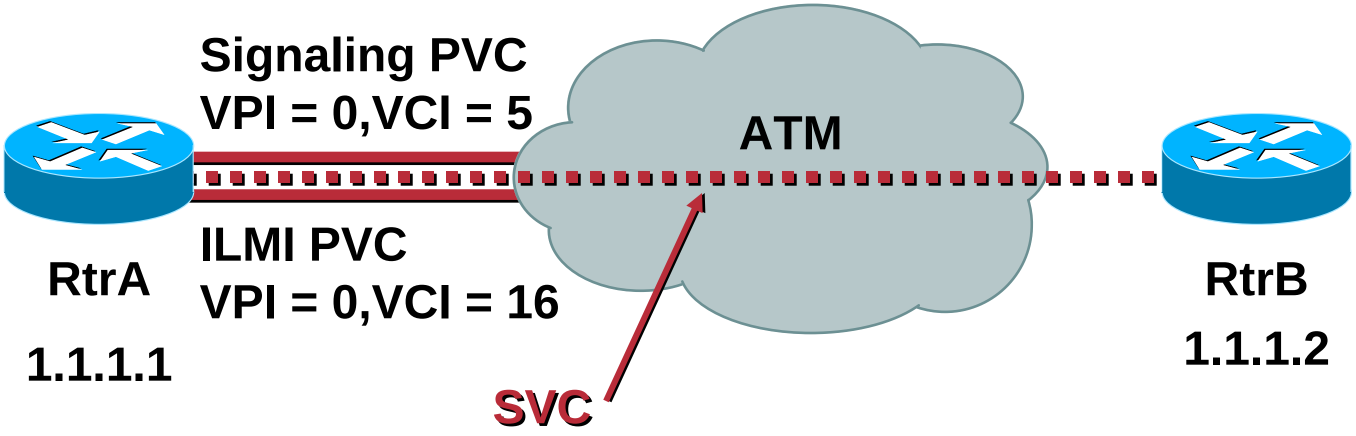
PVC Scenario (Cont.)

Verifying PVC Setup

```
RtrA#show atm vc
                VCD/                                          Peak  Avg/Min Burst
Interface  Name    VPI    VCI   Type   Encaps    SC     Kbps    Kbps  Cells   Sts
3/0.1         1       0     108   PVC     SNAP    UBR  155000                  UP
```

ATM SVC Setup

NSAP Address: 47.0091810000000001007386901.777777777777.00



ATM SVC Setup (Cont.)

- **Using SVC's requires the signaling and ILMI PVC's**
- **Station addressing uses 20-byte NSAP addresses**
- **Use *show atm ilmi-status* to check ILMI**
- **Use *debug atm sig-events* to check signaling**

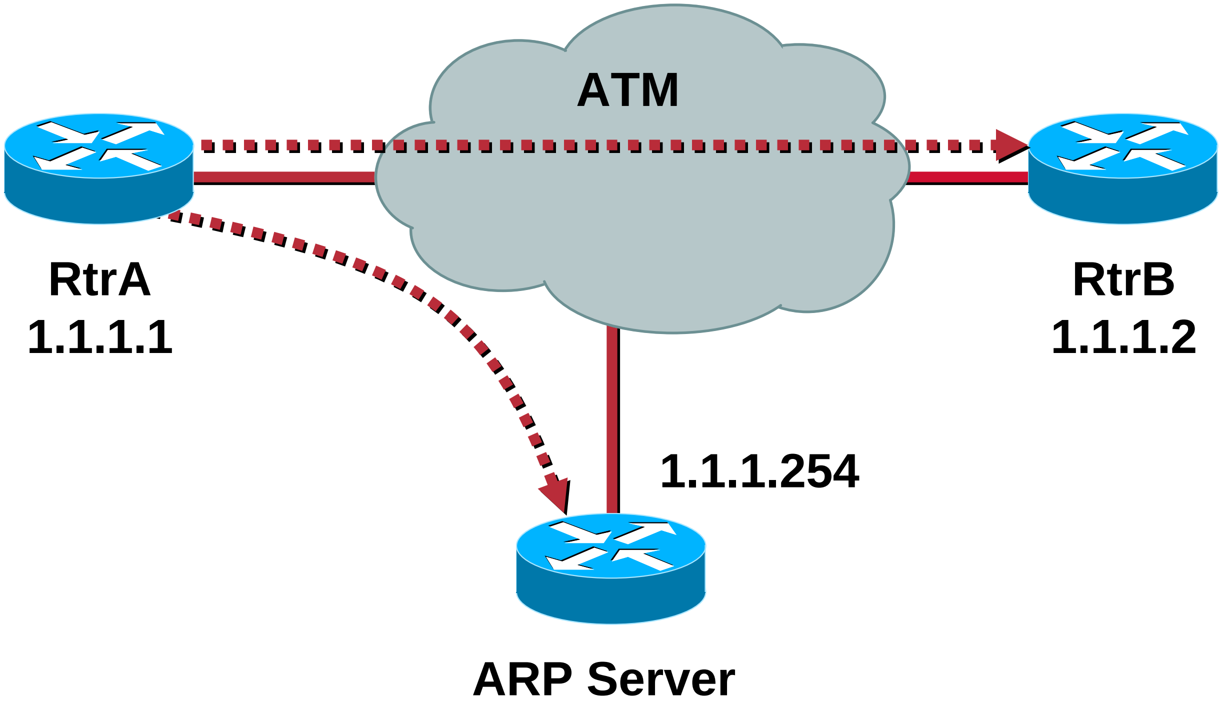
Classical IP-over-ATM

Cisco.com

Step 1: RtrA Wants to Ping 1.1.1.2

Step 2: RtrA Asks ARP Server for NSAP Matching 1.1.1.2

Step 3: RtrA Creates SVC to RtrB's NSAP



Classical IP-over-ATM (Cont.)

End-Station Configuration Example

```
interface ATM3/0
 no ip address
 pvc 0/5 qsaal
 pvc 0/16 ilmi
!
!
interface ATM3/0.1 multipoint
 ip address 1.1.1.1 255.255.255.0
 atm esi-address 777777777777.00
 atm arp-server nsap 47.009181000000001007386901.555555555555.00
```

Signaling and ILMI PVC’s

ESI for this End-Station

Full NSAP of arp Server

Classical IP-over-ATM (Cont.)

Checking End-Station Connectivity

```
RtrA#show arp
Protocol Address    Age (min)   Hardware   Addr Type    Interface
Internet 1.1.1.2        0         0/55        ATM        ATM3/0.1
Internet 1.1.1.1        0         0/54        ATM        ATM3/0.1
```

ATM Feature Example

- Setting the Service Class of a PVC using the VC-Class mechanism

```
hostname RtrA
!
interface ATM3/0.1 point-to-point
 ip address 1.1.1.1 255.255.255.0
 pvc 0/108
  class-vc vclass
  protocol ip 1.1.1.2
  encapsulation aal5snap
 !
vc-class atm vclass
  abr 1000 0
```

Apply VC-Class to PVC

VC-Class Setting Service Parameters

Preparing and Implementing ATM

- An ATM switch is required to practice SVC-based scenarios; the switch can also be used for various server functions in a test setup
- Classify a test question as a PVC or Classical IP-over-ATM question before you start

Preparing and Implementing ATM (Cont.)

- **References**

  ATM Resource Library, Volumes 1, 2 and 3 (Black, Prentice Hall)

  http://www.cisco.com/warp/public/121/index.shtml

  CiscoCD—Internetworking Design Guide—ATM

  CiscoCD—Configuration and Command References

Security

Security Topics—
Routing and Switching

- Using IP Access Lists
- Advanced IP Access List Example
- Catalyst Security
- Preparation and Implementation

Using IP Access Lists

- Two types: basic and extended

```
access-list 2 permit 1.1.1.0 0.0.0.255
access-list 100 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0 eq 23
```

- List elements are applied in order

```
access-list 102 deny ip host 1.1.1.1 any
access-list 102 permit ip host 1.1.1.1 any
```

Using IP Access Lists (Cont.)

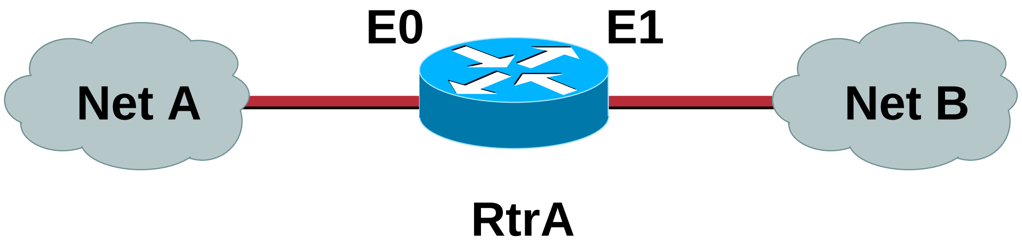
- **Implicit deny at end of list**

```
access-list 100 permit tcp host 1.1.1.1 any


access-list 100 permit tcp host 1.1.1.1 any
access-list 100 deny ip any any
```

- **Applied *inbound* or *outbound***

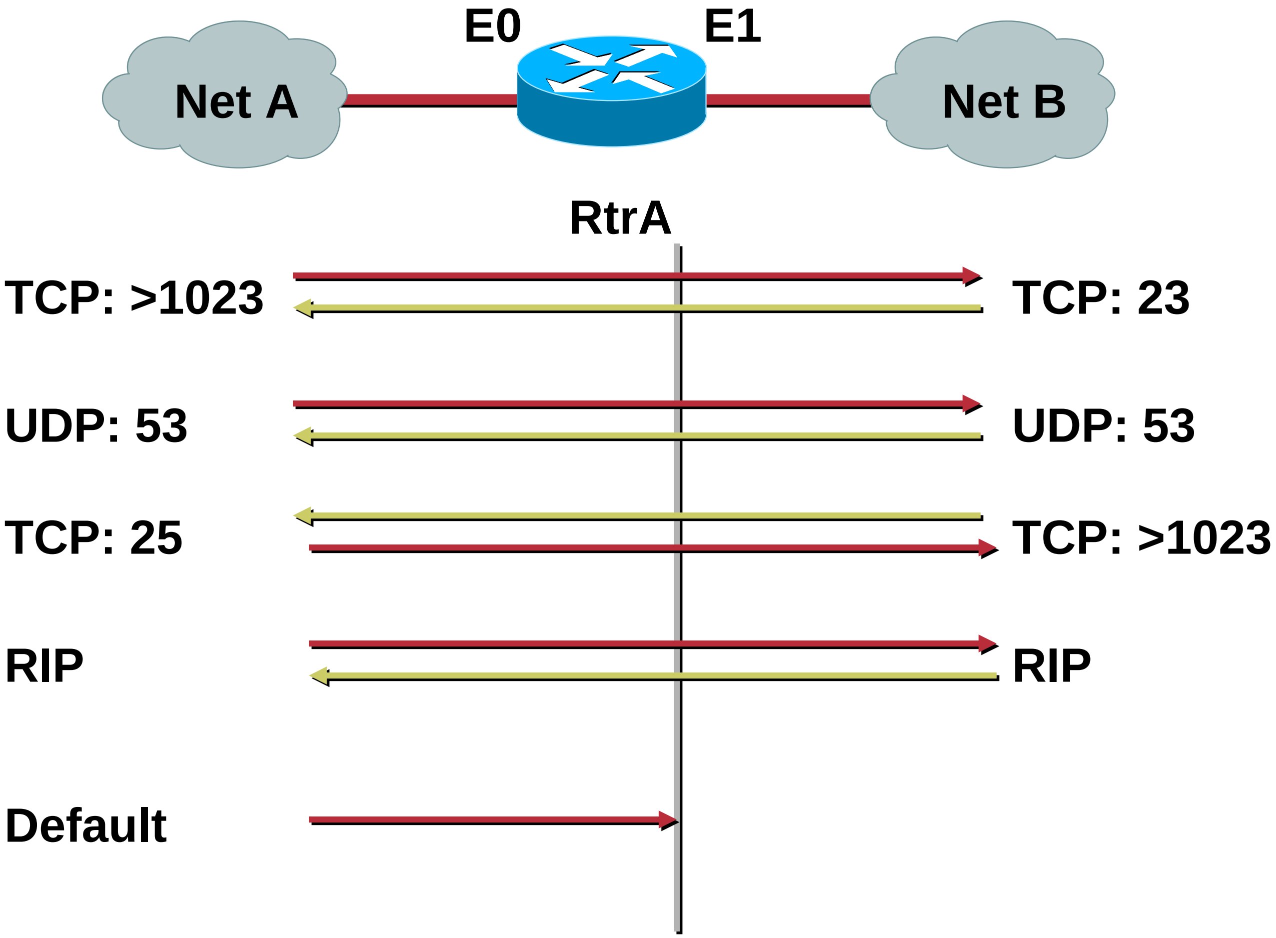
```
serial 0
 ip access-group 10 in
```

Access List Example



- **Apply an outgoing IP access list on Ethernet 1 of RtrA such that:**
  - **Telnet sessions originating on net A are allowed**
  - **DNS traffic is allowed**
  - **SMTP sessions originating on net B are allowed**
  - **Routing protocol traffic is permitted**
  - **All other traffic is denied**

Access List Example (Cont.)



E0

E1

Net A

Net B

RtrA

TCP: >1023

TCP: 23

UDP: 53

UDP: 53

TCP: 25

TCP: >1023

RIP

RIP

Default

Access List Example (Cont.)

```
interface  Ethernet 1
  ip access-group 100 out
!
!
access-list 100 permit tcp any any eq 23
access-list 100 permit udp any any eq 53
access-list 100 permit tcp any eq 25 any established
access-list 100 permit udp any any eq rip
```

(The Last Line Is Not Strictly Necessary Here)

Deny Martian and RFC 1918 Addresses

- RFC 1918 lists addresses known as private; no packet with such addresses should be on the Internet
- Beside RFC 1918 some addresses are currently not used or don’t make sense
  - IANA reserved
  - Test
  - Multicast as a source
  - Loopback netblocks

Deny Multicast Source and RFC 1918 Addresses

```
interface Serial 0/0
 ip access-group 111 in
!
access-list 111 deny ip 10.0.0.0 0.255.255.255 any
access-list 111 deny ip 172.16.0.0 0.15.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
…
access-list 111 deny ip 224.0.0.0 31.255.255.255 any
access-list 111 permit ip any any
```

Don't Forget the 'implicit deny'—No Points!

Unicast Reverse-Path Forwarding Checks

- Mitigates source address spoofing by checking that a packet's return path uses the same interface it arrived on
- Pay close attention to where implemented
- Requires CEF
- Not always appropriate where asymmetric paths exist

```
ip cef distributed
!
interface Serial 0
  ip verify unicast reverse-path
```

CAR for Security

```
interface Serial 0/0
   rate-limit output access-group 102 64000 2000 2000
   conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

- Limits ping ‘flooding’ to specified rate
- Same configuration required on adjacent router in other direction? (inbound)

Debugging Access Lists

- **show access-lists** can provide traffic information on ACL's:

```
RtrA#sh access-lists
Extended IP access list 100
    permit tcp any any eq telnet (10 matches)
    permit udp any any eq domain
    permit tcp any eq smtp any established (1 match)
    permit udp any any eq rip
```

Debugging Access Lists (Cont.)

- **Adding the *log* keyword provides more information**

```
access-list 100 permit tcp any any eq telnet log
access-list 100 permit udp any any eq domain log
access-list 100 permit tcp any eq smtp any established log
access-list 100 permit udp any any eq rip log
access-list 100 deny   ip any any
```

```
%SEC-6-IPACCESSLOGP: list 100 permitted tcp 1.1.1.1(11003) ->
4.4.4.4(23), 1 packet
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 1.1.1.1 -> 4.4.4.4
(8/0), 5 packets
```

Implementation Suggestions

- Draw a diagram showing required traffic through the ACL
- Watch the order of list elements, and the logic
- If all or part of the list can be tested, make sure you do!
- Check routing after applying the list

Implementation Suggestions (Cont.)

- **Don't forget the "deny all" at the end of the list**

5.1 Deny all IP traffic to host 1.1.1.1

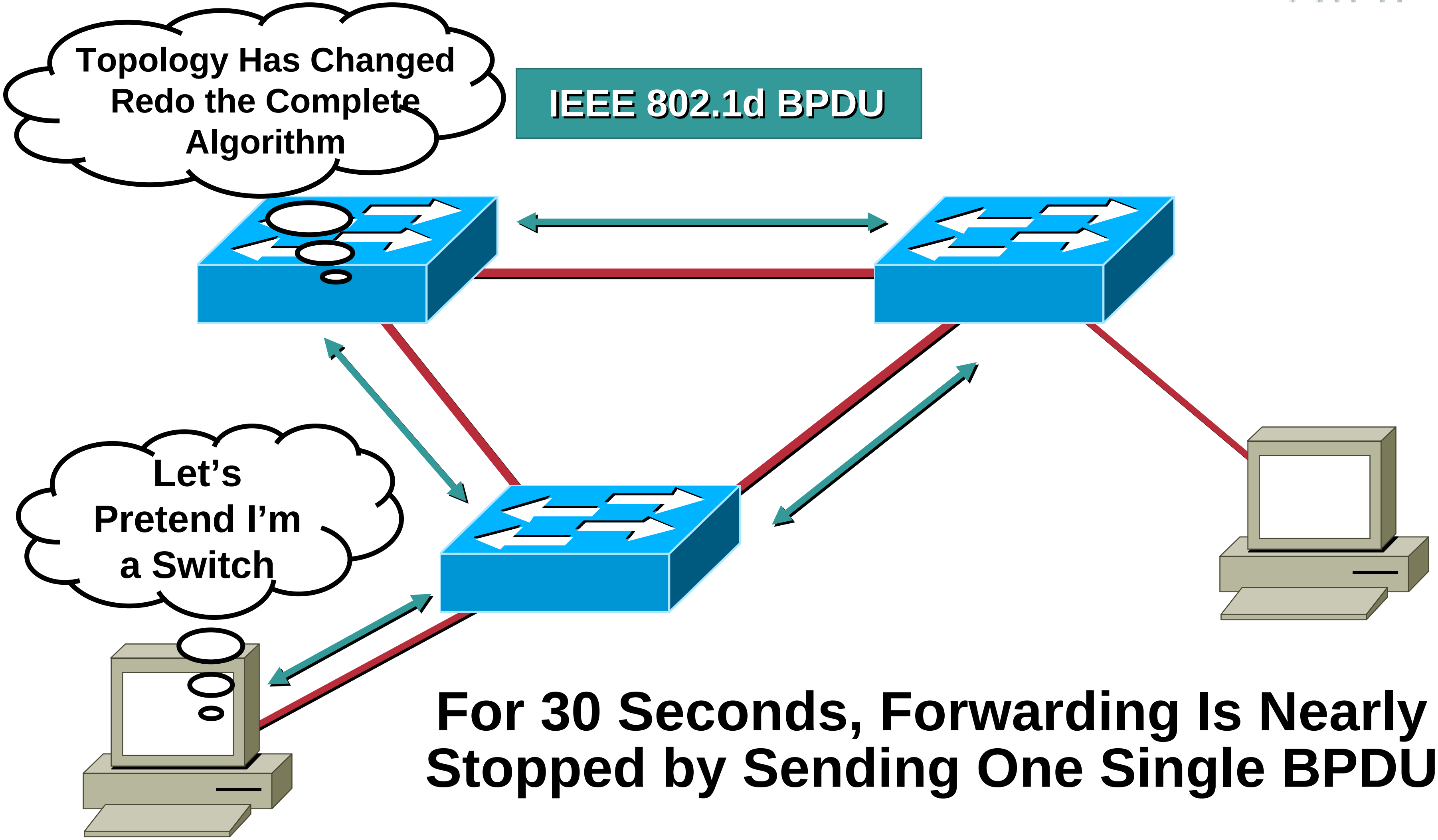
Incorrect:

```
access-list 100 deny ip any host 1.1.1.1
```

Correct:

```
access-list 100 deny ip any host 1.1.1.1
access-list 100 permit ip any any
```

Catalyst Security—BPDU/Root Guard



For 30 Seconds, Forwarding Is Nearly Stopped by Sending One Single BPDU

Catalyst Security—BPDU/Root Guard

- It is possible to disable STP in loop free topologies but the test may not permit this; by default spanning tree is enabled on all VLANs
- BPDU guard

  Enable globally and set the port configuration as the default for BPDU guard

  Use PortFast to enable or disable BPDU guard

  Disables ports upon detection of a BPDU message on the port
- Root guard

  Forces a port to become a designated port so that no switch on the other end of the link can become a root switch

BPDU Guard—Sample Configuration

```
Switch(config)# spanning-tree portfast bpduguard
    Switch(config-if)# spanning-port portfast
    Switch(config)# spanning-tree guard root (or rootguard)
```

NOTE: Global Configuration

Preparation Suggestions

- **Know some standard port numbers and protocol behaviors**
- **Practice using access lists you can actually test**

Preparation Suggestions (Cont.)

- References

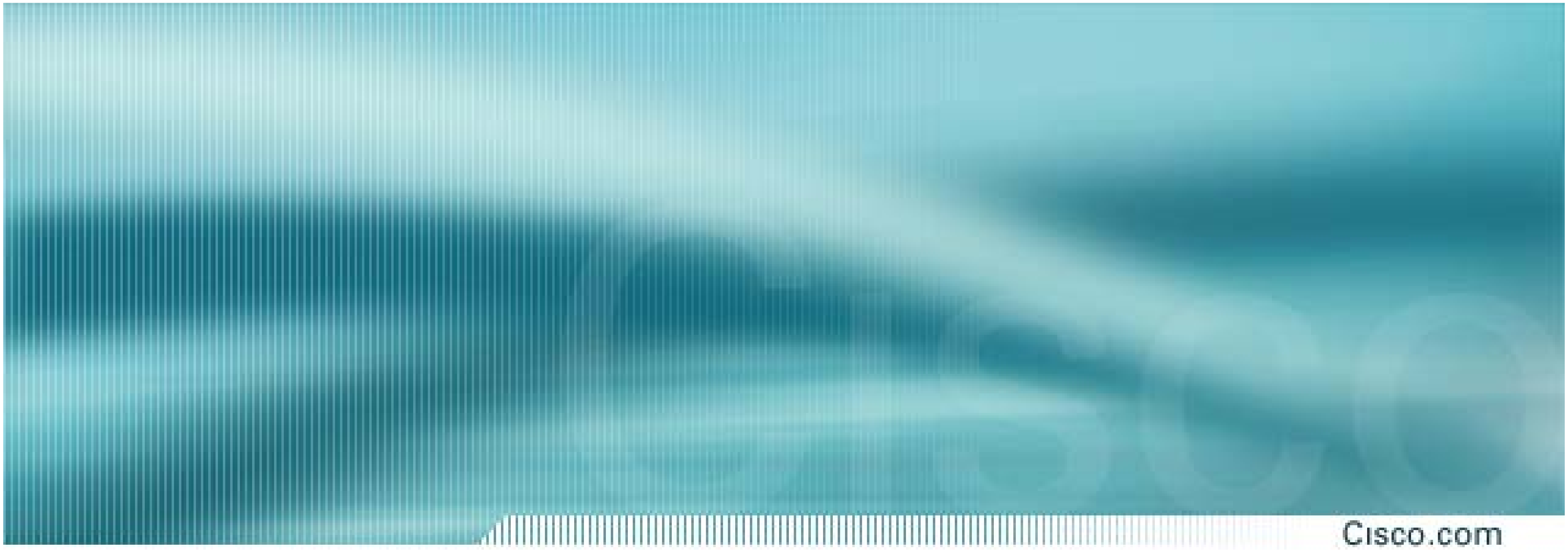
  http://www.cisco.com/warp/public/707/index.shtml

  Designing Network Security (Kaeo, Cisco Press)

  Enhanced IP Services for Cisco Networks (Lee, Cisco Press)

  CiscoCD—Internetworking Design Guide—Security

  CiscoCD—Configuration and Command References



Questions?

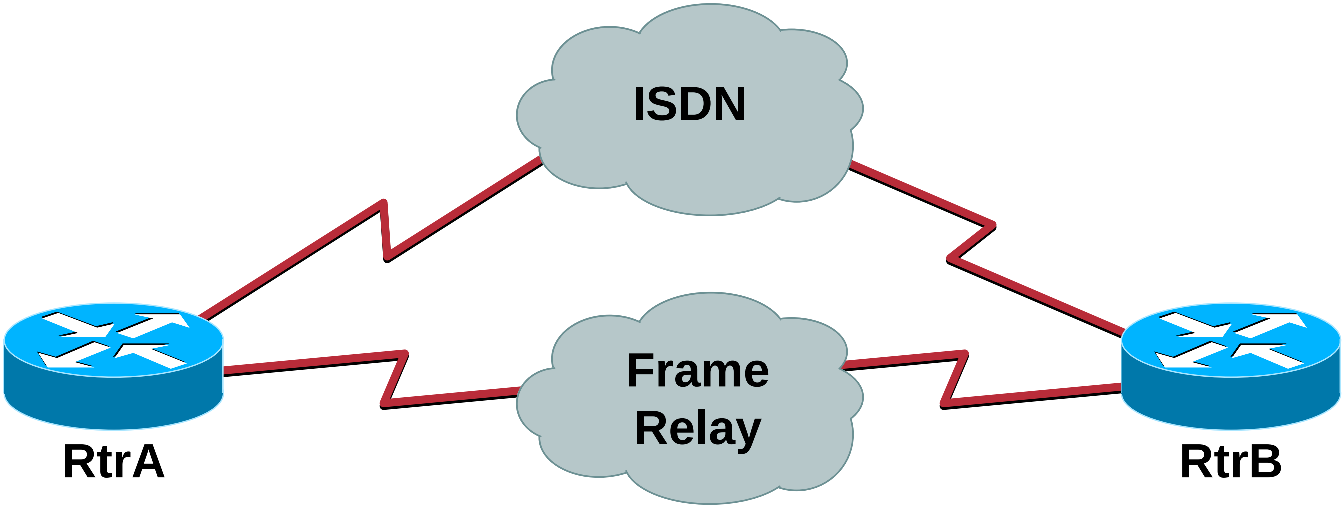
Section 7

ISDN and Dial Features

ISDN and DDR

- Basic Configuration-Provided
- Debugging ISDN
- Authentication and Multilink
- DDR Scenarios
- Preparing for ISDN

Basic Setup



Common Test Scenario

Basics—Legacy DDR

```
hostname RtrA
!
enable password cisco
!
username RtrB password 0 cisco
!
interface BRI0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
 dialer map ip 1.1.1.2 name RtrB broadcast 1113333
 dialer-group 1
 isdn switch-type basic-dms100
 isdn spid1 902111222200 1112222
 isdn spid2 902111222301 1112222
 ppp authentication chap
!
dialer-list 1 protocol ip permit
```

Authentication Info—RtrA

Authentication Info—RtrB

Link Encapsulation Format

Local IP

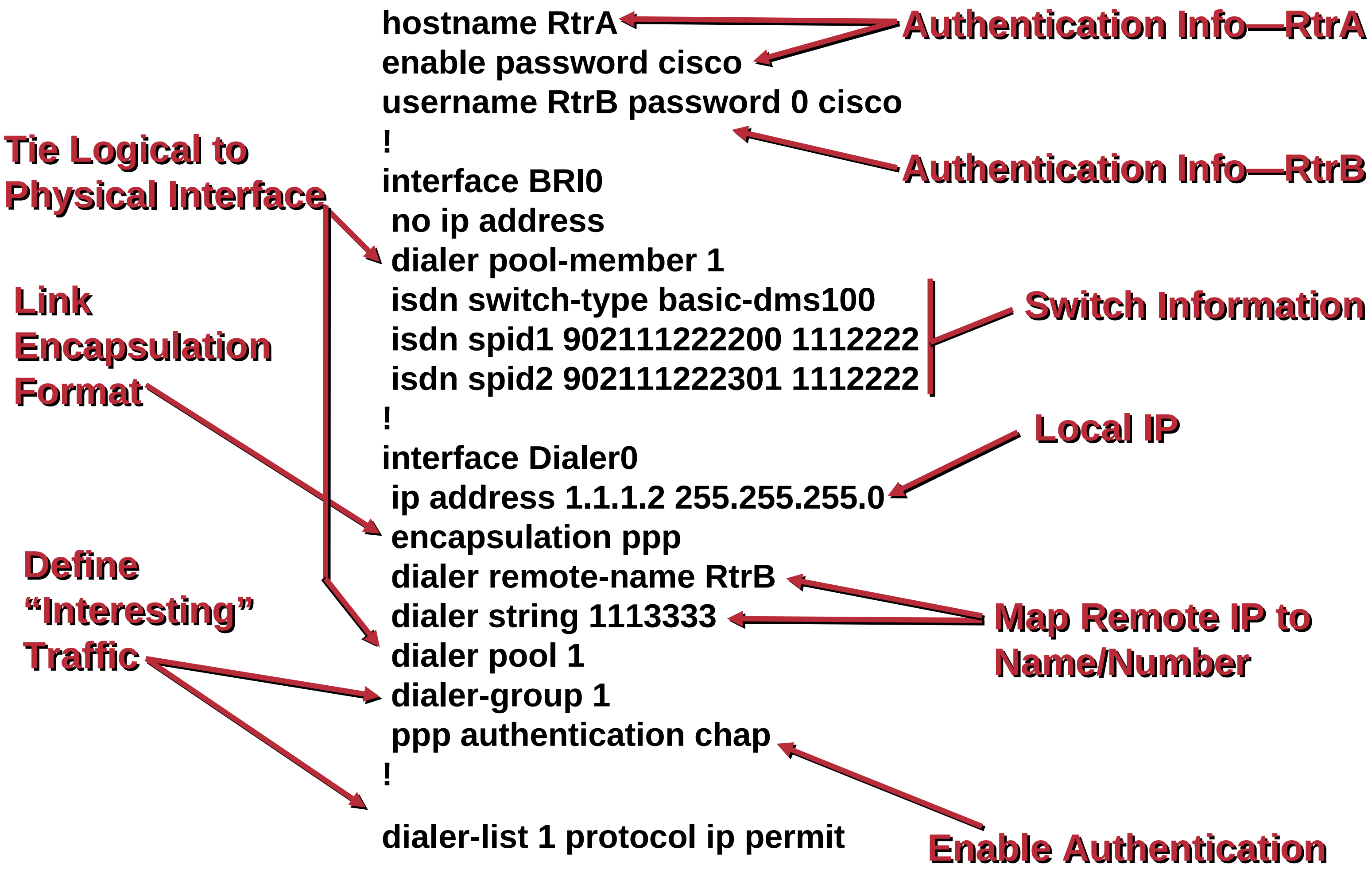
Define “Interesting” Traffic

Map Remote IP to Name/Number

Switch Information

Enable Authentication

Basics—Profiles



```
hostname RtrA
enable password cisco
username RtrB password 0 cisco
!
interface BRI0
 no ip address
 dialer pool-member 1
 isdn switch-type basic-dms100
 isdn spid1 902111222200 1112222
 isdn spid2 902111222301 1112222
!
interface Dialer0
 ip address 1.1.1.2 255.255.255.0
 encapsulation ppp
 dialer remote-name RtrB
 dialer string 1113333
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!

dialer-list 1 protocol ip permit
```

Authentication Info—RtrA

Authentication Info—RtrB

Tie Logical to Physical Interface

Link Encapsulation Format

Switch Information

Local IP

Define “Interesting” Traffic

Map Remote IP to Name/Number

Enable Authentication

Debugging—Basic Connectivity

show isdn status

```
The current ISDN Switchtype = basic-dms100
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 68, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 70, State = MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
        TEI 68, ces = 1, state = 8(established)
            spid1 configured, spid1 sent, spid1 valid
            Endpoint ID Info: epsf = 0, usid = 70, tid = 0
        TEI 70, ces = 2, state = 8(established)
            spid2 configured, spid2 sent, spid2 valid
            Endpoint ID Info: epsf = 0, usid = 71, tid = 0
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs = 0
```

Debugging—Call Progress

debug dialer, debug isdn events

```
08:45:08: BRI0 DDR: rotor dialout [priority]
08:45:08: BRI0 DDR: Dialing cause ip (s=1.1.1.2, d=1.1.1.1)
08:45:08: BRI0 DDR: Attempting to dial 1112222
08:45:08: ISDN BRI0: Outgoing call id = 0x800F, dsl 24
08:45:08: ISDN BRI0: Event: Call to 1112222 at 64 Kb/s
08:45:08: ISDN BRI0: process_bri_call(): call id 0x800F, called_number 1112222,
 speed 64, call type DATA
08:45:08: CC_CHAN_GetIdleChanbri: dsl 24
08:45:08:     Found idle channel B1
08:45:08: ISDN BRI0: received HOST_PROCEEDING call_id 0x800F
08:45:09: ISDN BRI0: received HOST_CONNECT call_id 0x800F
08:45:09: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
08:45:09: BRI0:1: interface must be fifo queue, force fifo
08:45:09: %DIALER-6-BIND: Interface BRI0:1 bound to profile Dialer0
08:45:09: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 1112222
08:45:09: isdn_call_connect: Calling lineaction of BRI0:1
08:45:09: ISDN BRI0: Event: Connected to 1112222 on B1 at 64 Kb/s
```

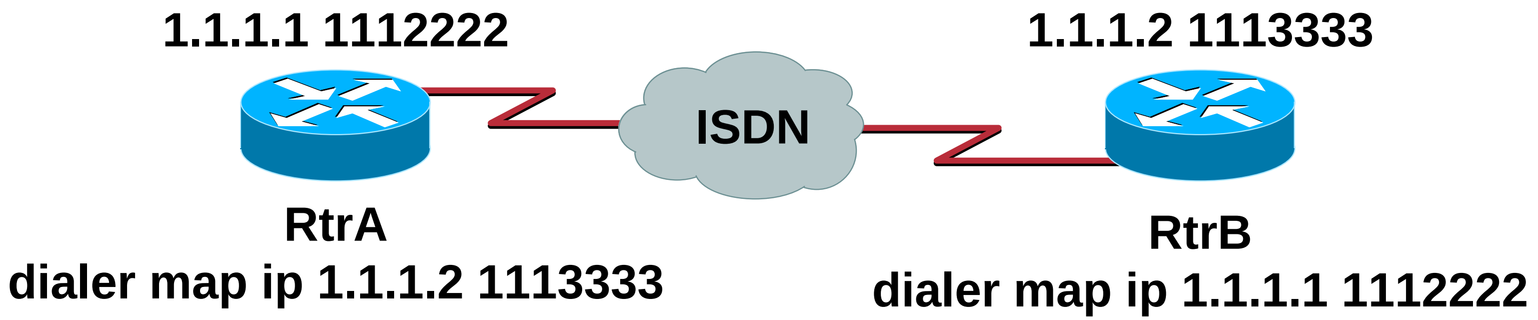
Other Debugging Commands

- **PPP:** ***debug ppp negotiation, debug ppp authentication***
- **IP problems:** ***debug ip packet***
- **More detailed call progress (as a last resort):** ***debug isdn q931, debug isdn q921***

Authentication

- Authentication verifies the identity of a remote host
- Authentication is also part of calling and routing with ISDN

ISDN without Authentication


1.1.1.1 1112222

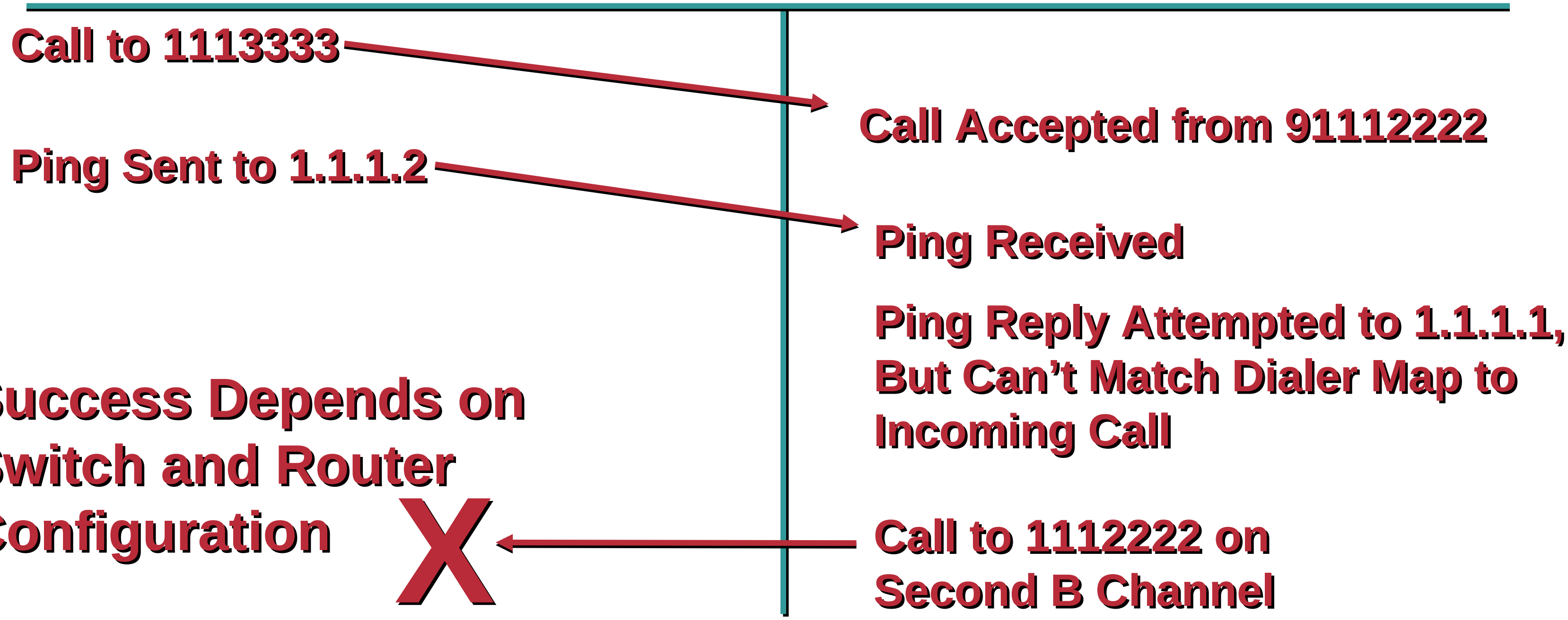
1.1.1.2 1113333

RtrA

dialer map ip 1.1.1.2 1113333

RtrB

dialer map ip 1.1.1.1 1112222


Call to 1113333

Call Accepted from 91112222

Ping Sent to 1.1.1.2

Ping Received

Ping Reply Attempted to 1.1.1.1, But Can't Match Dialer Map to Incoming Call

Call to 1112222 on Second B Channel

X

Success Depends on Switch and Router Configuration

ISDN without Authentication (Cont.)

- Can depend on router and telco switch configuration
- Creates two unidirectional channels—i.e. uses half the bandwidth

ISDN with Authentication

1.1.1.1 1112222

RtrA
dialer map ip name RtrA
1.1.1.2 1113333

1.1.1.2 1113333

RtrB
dialer map ip name RtrB
1.1.1.1 1112222

Call to 1113333 (RtrB) → **Call Accepted from 91112222 (RtrA)**

Ping Sent to 1.1.1.2 → **Ping Received**

Ping Reply Attempted to 1.1.1.1; Dialer Map Matches "RtrA" to Existing Call

Ping Reply Received ← **Ping Reply Sent to 1.1.1.1 Over Existing Channel**

ISDN with Authentication

- Less sensitive to telco switch configuration
- More reliable in test situations
- Allows full use of ISDN bandwidth

PPP Feature Example

- **Implementation of Multilink PPP with both channels; this task requires:**
  - authentication
  - Local Directory Numbers (LDN's) on SPID's
  - a second dialer map or string
  - ppp multilink command—to create bundles
  - dialer load-threshold command, to bring up second channel
  - show ppp multilink shows:

```
Dialer0, bundle name is RtrA
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x6/0x6
rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member links: 2 (max not set, min not set)
    BRI0:1
    BRI0:2
```

DDR Techniques

- **Floating static routes**
- **Dial backup**
- **Dialer watch**
- **OSPF demand circuit**

Floating Static Routes

`ip route 2.2.2.0 255.255.255.0 1.1.1.2 240`

- Uses a higher administrative distance so that dynamic protocols will take precedence
- Use only if explicitly allowed in a test question
- Make sure the dynamic route actually exists when DDR is not active

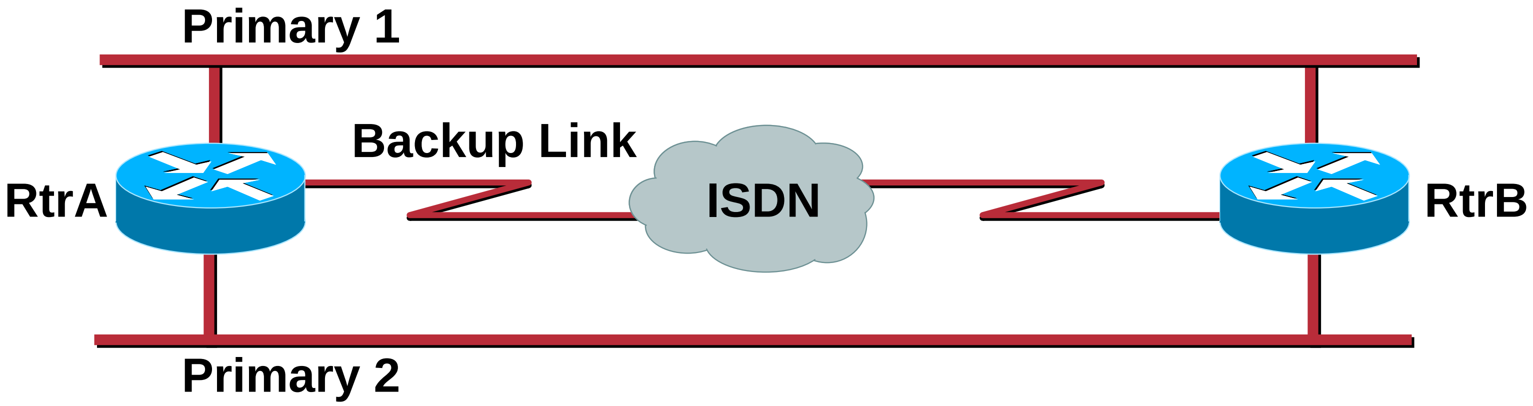
Dial Backup

```
interface Serial0
 backup delay 10 10
 backup interface Dialer0
```

- Use if the backup link can be tied to a physical interface
- Use it to trigger one end of a backup link or the other—not both!
- When the bri is a backup to a primary interface, the actual interface must be down (not administratively down) as well as the line protocol

Dialer Watch

Cisco.com



- Allows a backup link to support multiple primary links
- Monitors specific network addresses

Dialer Watch (Cont.)

```
hostname RtrA
!
interface BRI0
 ip address 1.1.1.1 255.255.255.0
 encapsulation ppp
 dialer map ip 1.1.1.2 name RtrB broadcast 1113333
 dialer map ip 1.1.2.0 name RtrB broadcast 1113333
 dialer map ip 1.1.3.0 name RtrB broadcast 1113333
 dialer-group 1
 dialer watch-group 2
 isdn switch-type basic-dms100
 isdn spid1 902111222200 1112222
 isdn spid2 902111222301 1112222
 ppp authentication chap
!
access-list 101 deny eigrp any any
access-list 101 permit ip any any
dialer watch-list 2 ip 1.1.2.0 255.255.255.0
dialer watch-list 2 ip 1.1.3.0 255.255.255.0
dialer-list 1 protocol ip list 101
```

Dialer Watch (Cont.)

- Dialer Watch will keep the backup interface down until the monitored route(s) are no longer reachable through the primary interfaces
- Dialer Watch only supports IP, works best with EIGRP but is supported for OSPF and IGRP

OSPF Demand Circuit

- **Useful if the backup link and failure point are in different parts of your network**
- **Suppresses OSPF HELLO and Refresh LSA's and keeps routes visible even if the backup link drops**
- **Can be difficult to implement**

OSPF Demand Circuit (Cont.)

- **Suggestions for use:**
  - **Configure on one side of the link only**
  - **Don’t change the OSPF network type of the backup link**
  - **Make sure the question permits the link to come up for topology changes**
  - **Watch for routing loops**
  - **Increase the OSPF cost value of the ISDN link so that the preferred path is always the primary link**

OSPF Demand Circuit (Cont.)

Routing Loop Example:

```
interface BRI0
 ip address 1.1.1.1 255.255.255.0
 ip ospf demand-circuit
!
router ospf 10
 redistribute rip subnets
 network 1.1.1.1 0.0.0.0 area 5
!
router rip
 redistribute connected
 redistribute ospf 10
 network 3.0.0.0
 default-metric 3
```

Preparation Suggestions

- **ISDN requires hands-on practice with both ends of a link**
- **The debug and show commands produce lots of output—you need to learn what’s normal and what’s unusual**

References

- ISDN and SS7: Architectures for Digital Signaling Networks (Black, Prentice Hall)
- Cisco Interactive Mentor, Multiprotocol Challenge, Cisco Press
- Building Cisco Remote Access Networks (Paquet, Cisco Press)
- http://www.cisco.com/warp/public/471/index.shtml
- CiscoCD—Internetworking Design Guide
- CiscoCD—Dial Solutions Quick Configuration Guide
- CiscoCD—Configuration and Command References

Implementation Suggestions

- Start with “minimal” configuration
- Use authentication!
- Read any DDR scenario carefully
- Watch for “typing errors”
- Switch types vary from site to site

Implementation Suggestions (Cont.)

- Debug from the bottom up—check:
    - Connection with the switch
    - Call progress
    - PPP and authentication
    - IP connectivity
- Leave a working configuration

Questions?

Session 8

Preparation, and Questions

Topics

- Preparing for the Exam
- Test-Taking Strategies
- Information Sources

Exam Preparation

- The qualification test
- Assessing strengths and weaknesses
- Materials and resources
- Practicing

The Qualification Test

- Use the content blueprint on the CCIE Web page as your guide
- The reading list materials are suggestions only
- The test stresses networking theory more than configuration skill
- Don’t study for the qualification test and the lab at the same time

Assessing Strengths

- Using the content blueprint, determine your experience and knowledge level in the major topic areas
- For strength areas, practicing for speed should be sufficient
- For weak areas, you may need training or books in addition to practice

Materials and Resources

- **For the lab exam, choose materials that provide configuration examples and take a “hands-on” approach**
- **Know the Cisco documentation CD**

Practicing

- Find equipment
- Build and practice scenarios on a per topic basis
- Go beyond the basics—practice additional features
- Learn show and debug commands along with each topic

Practicing (Cont.)

- If a protocol has multiple ways of configuring a feature, practice all of them
- Speed is vital on the exam; review and practice core material (Frame Relay, OSPF, BGP, basic ISDN) the week before your exam date

Test-Taking Strategies

- **Arrive early or visit the site the day before**
- **Don’t schedule flights too close to the end of the exam—it can run overtime**
- **Get some sleep the night before the exam**

Test-Taking Strategies (Cont.)

- Use question point values to judge time
- Read through the entire test first to check for addressing issues

Test-Taking Strategies (Cont.)

- Do each question as a unit—configure and verify before moving to the next question
- Don’t assume requirements that aren’t mentioned in a question
- Don’t make any drastic changes in the last half hour of the exam
- Save your configs often

Test-Taking Strategies (Cont.)

Ask the Proctor Questions

Test-Taking Strategies (Cont.)

- The proctor’s role is to keep the exam as fair as possible; you should talk to the proctor if you don’t understand a question, or if you experience technical problems

For More Information…

- **Beware of rumors!**
- **Visit the CCIE web page at**

  www.cisco.com/go/ccie
- **Email: ccie@cisco.com**
- **Cheating:**

  ccie-nda-enforcement@cisco.com

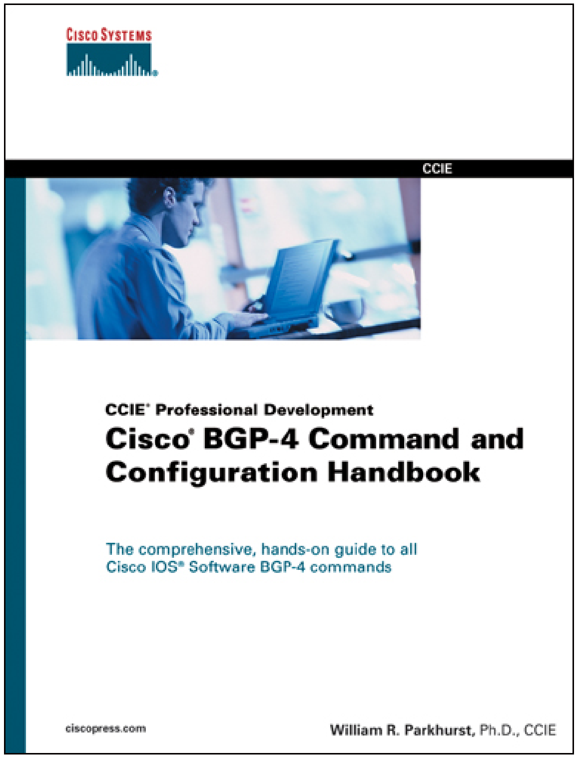
Questions?

Recommended Reading

BGP-4 Command and Configuration Handbook
ISBN: 158705017X

Cisco OSPF Command and Configuration Handbook
ISBN: 1587050714

CCIE Practical Studies, Vol I
ISBN: 1587200023



Available on-site at the Cisco Company Store

Recommended Reading

CCIE Routing and Switching Exam Certification Guide

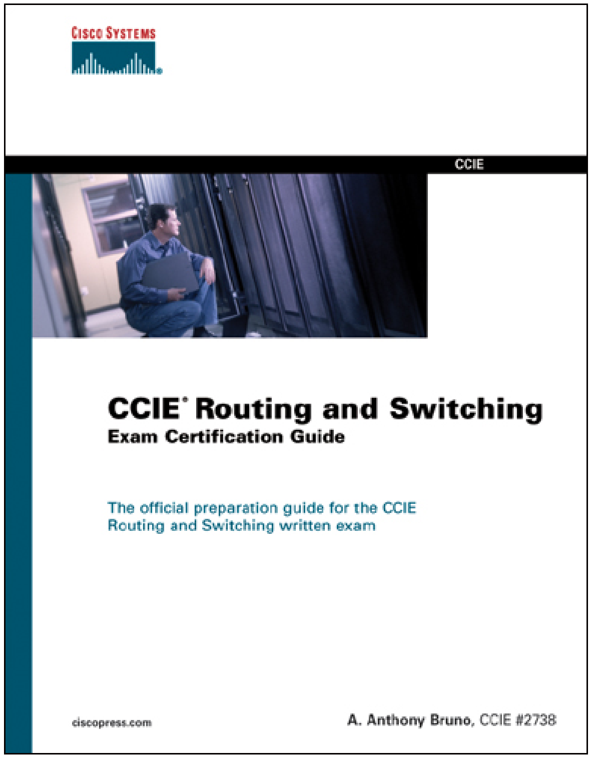
ISBN: 1587200538

CCIE Practical Studies: Security

ISBN: 1587051109

CCIE Security Exam Certification Guide

ISBN: 1587200651



Cisco Systems

CCIE

CCIE® Routing and Switching
Exam Certification Guide

The official preparation guide for the CCIE
Routing and Switching written exam

ciscopress.com

A. Anthony Bruno, CCIE #2738

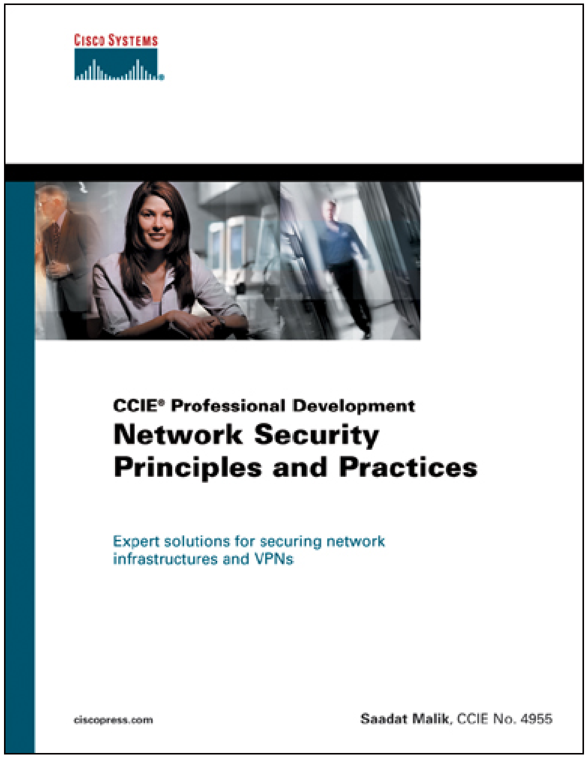
Available on-site at the Cisco Company Store

Recommended Reading

Network Security Principles and Practicies
ISBN: 1587050250

Troubleshooting Remote Access Enterprise Networks
ISBN: 1587050765

Troubleshooting IP Routing Protocols
ISBN: 1587050196



CISCO SYSTEMS

CCIE® Professional Development
Network Security Principles and Practices

Expert solutions for securing network infrastructures and VPNs

ciscopress.com

Saadat Malik, CCIE No. 4955

Available on-site at the Cisco Company Store

Recommended Reading

Routing TCP/IP Vol. I

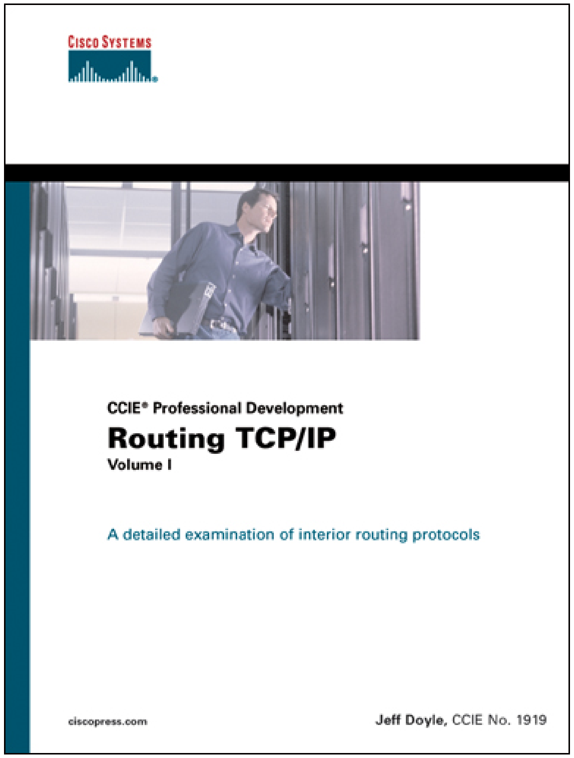
ISBN: 1578700418

Routing TCP/IP Vol II

ISBN: 1578700892

Cisco LAN Switching

ISBN: 1578700949



CISCO SYSTEMS

CCIE® Professional Development

Routing TCP/IP

Volume I

A detailed examination of interior routing protocols

ciscopress.com

Jeff Doyle, CCIE No. 1919

Available on-site at the Cisco Company Store

NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Please Complete Your Evaluation Form

Session PWR-5014

CISCO SYSTEMS

CISCO SYSTEMS