Asia Pacific Network Information Centre

APNIC

Welcome!
APNIC Workshop

Routing Essential

Aug 30 – Sept 1, 2005, Hanoi Vietnam

Asia Pacific Network Information Centre

APNIC

Schedule (Day 1)

- Introduction
- Routing Principles
- IP fundamentals

TEA BREAK
(10:30 – 11:00)

- IP addressing
- Network planning essentials

LUNCH (12:30 – 13:30)

- Router configuration requirements
- Written exercise

TEA BREAK
(15:30 – 16:00)

- Hands-on exercise (Router initial configuration)

Asia Pacific Network Information Centre

APNIC

Schedule (Day 2)

- Configuring OSPF in a single area
- Written exercise

TEA BREAK
(10:30 – 11:00)

- Labs - Configuring Static route

LUNCH (12:30 – 13:30)

- Labs - Configuring Default route

TEA BREAK
(15:30 – 16:00)

- Written exercise

Schedule (Day 3)

- Configuring BGP
- Written exercise

TEA BREAK (10:30 – 11:00)

- Labs - Configuring iBGP

LUNCH (12:30 – 13:30)

- Labs - eBGP

TEA BREAK (15:30 – 16:00)

- Labs – Combining OSPF and BGP

Routing Workshop

Routing essentials

Introduction to routing essentials

Overview

- Course objectives
- Course topics
- Prerequisites
- Participants role during the training
- Course contents
- Graphics / symbols used
- Introduction to lab scenario
- Information sources

Course objectives

- To gain the appropriate foundation knowledge and to be able perform the following:
  - Identify and differentiate routing protocols (RIP,OSPF, ISIS, BGP)
  - Simplify and manage addressing calculation effectively
  - Define each network layers to attain hierarchical addressing right protocol usage

Course objectives (cont.)

- Configure and perform initial router configuration requirements
- Configure OSPF in a single area and interconnect multi-area OSPF network
- Build and network running both OSPF and BGP protocol

Course topics

- The course focus is to building a start-up network with focus to configuring the following in a network devices.
  - TCP/IP protocols and IP addresses
  - VLSM and route summarisation
  - OSPF and BGP protocol
  - Route announcements
  - Router interfaces configuration
  - Peering connection within and outside the network

Prerequisites

- Understand the use of commonly used networking terms
- Open Systems Interconnection (OSI) reference model
- Knowledge about distance vector protocols operation and configuration
- Able to perform basic TCP/IP troubleshooting (ping and traceroute)

Participants role during the training

- Meet all the required prerequisites
- Able to understand clearly the topics discussed
- Turn-off or silent mode mobile phones
- Ask and answers questions

Self introduction

- Name and work location
- Job description
- Internetworking experience (if any)
- Expectation about the course

Course contents

- Introduction
- Routing principles
- IP addressing
- Network planning essentials
- Router configuration requirements
- Configuring OSPF in a single area
- Configuring BGP
- Summary

Graphics / symbols used


Router
(layer 3, IP datagram forwarding)


Network Access Server
(layer 3, IP datagram forwarding)


Ethernet switch
(layer 2, packet forwarding)

Introduction to lab scenario

- During the entire duration of the course there will a hands-on lab exercises created to perform the actual configuration requirements.
- There will be different sets of sample scenarios to gain practical experience on how it works in a network environment.

Information sources

- Student kit
  - Presentation manual
  - Exercises manual
    - Written exercises
    - Lab exercises
  - Information sources
    - www.ietf.org
    - www.cisco.com

Questions?

Routing principles

Overview

- Routing fundamentals
- Routing protocol distinctions
  - Classful routing (obsolete)
  - Classless routing
  - Distance Vector
  - Link-state
- Written exercises: Routing protocols comparison
- Summary

Objectives

- To be able to gain knowledge about the foundation of the routing protocols
- Classify the difference between a classful and classless routing architecture
- Compare distance vector and link-state protocol operation
- Describe the information written inside the routing table

Routing fundamentals

What is a routing protocol?

- A set of rules defined to facilitate the exchanges of routing information between networks, allowing routers (Layer 3 device) to build routing tables dynamically to let the route find its path in a network having more than one path to a remote network.
- It also maintains the devices connectivity by sending updates to each devices within the network about the available network connections.

Routing protocol behaviour

- Mechanism to update Layer 3 routing devices, to route the data across the best path
- Learns participating routers advertised routes to know their neighbors
- Learned routes are stored inside the routing table

What is routing?

- Is the method of delivering an item from one location to another
  - Example Post Mail = delivery is being done via Port Office
- But in a router network environment what it does is to forward traffic to a logical device destination interface
- And routers perform two things to deliver the packets to its destination
  - 1st is Learning the logical topology of the network to store the path inside the routing table to where the traffic should flow which called “Routing”
  - 2nd is forwarding those packets learned from an inbound interface to the outbound interface within the router which is called “Switching”

Distinction between *routed* and *routing* protocols

- Routed protocols
  - Is a Layer3 datagram that carry the information required for transporting the data from one end to another across the network
- Routing protocols
  - Handles the updating requirement of the routers within the network for determining the path of the datagram across the network

Routing and *routed* protocols

Routed protocol	Routing protocol
AppleTalk	RTMP, AURP, EIGRP
IPX	RIP, NLSP, EIGRP
Vines	RTP
DecNet IV	DecNet
IP	RIPv2, OSPF, IS-IS, and (Cisco Systems proprietary) EIGRP, BGP

Routing requirements

- Activation of the protocol suite from such device participating the network
- Knowledge of the network destination
  - Must have available entry in the routing table
  - Must have valid and current route entry
- Interface presenting the best route path
  - Outbound interface with the lowest metric path

Routing information

- Routing table information
  - Network field
  - Outgoing interface
  - Metric field
  - Next1 Hop field
- Routing table example

Network field

- Contains information of entries
  - Networks learned (destination logical network or subnets)
    - Manually (static or default routes)
    - Dynamically (learned from routing protocol as dynamic routes)
- Information recorded is the entry where to forward traffic to its destination when the datagram is received.

Outgoing interface field

- Interface to where the router sends the datagram
- Informs the administrator of interface where the update came through

Metric field

- To determine which path to use if there are multiple paths to the remote network
- Provide the value to select the best path
- But take note of the administrative distance selection process ☺

Routing protocol metrics

Routing protocol	Metric
RIPv2	Hop count
EIGRP	Bandwidth, delay, load, reliability, MTU
OSPF	Cost (the higher the bandwidth indicates a lowest cost)
IS-IS	Cost

Administrative distance

- Is the method used for selection of route priority of IP routing protocol, the lowest administrative distance is preferred
  - Manually entered routes are preferred from dynamically learned routes
    - Static routes
    - Default routes
  - Dynamically learned routes depend on the routing protocol metric calculation algorithm and default metrics values the smallest metric value are preferred

Administrative distance chart (Cisco)

Route sources	Default distance
Connected interface	**0**
Static route out an interface	**0**
Static route to a next hop	**1**
External BGP	**20**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
RIP v1, v2	**120**
EGP	**140**
Internal BGP	**200**
Unknown	**255**

Next hop field

- Destination address of the next forwarding router
  - Address of the next hop (outgoing interface) usually within the same subnet
  - iBGP (exemption to the rule)
- Identify the next hop so that the router can create the Layer2 frame with the destination address

Routing table sample (Cisco)

Cisco-router#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set ?????????????

202.41.143.0/24 is variably subnetted, 2 subnets, 2 masks
S 202.41.143.0/24 is directly connected, Null0
C 202.41.143.17/32 is directly connected, Loopback0
O E2 10.110.0.0 [110/5] via 10.119.254.6, 0:01:00, Ethernet2
O 10.67.10.0 [110/128] via 10.119.254.244, 0:02:22, Ethernet2
B 217.170.115.0/24 [20/0] via 12.123.29.249, 5d16h

Routing table updates

- Routing table entry accuracy is required make sure of the following:
  - Table entry are current and correct
  - New networks are inserted in the table
  - Best path is available to the reach the destination network
  - Alternative routes are available to reach the destination network
  - Network that is no longer available should be removed in the routing table
- Depends on the routing protocol

Routing decisions

- The main goal of the routing decision is to maintain a valid and free from routing loop to the destination network regardless of whether it is single path or multiple path
- The decision is made base on the metric value in the routing table which is the sum of the metrics associated with the default routing protocol value and the intermediate connections

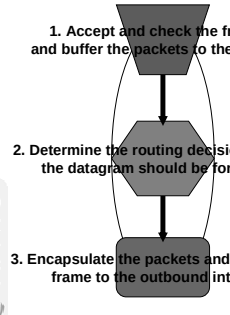
Switching and routing function

Routing function	Switching function
Learn the logical topology	Move data from the incoming to the outgoing router interface
Perform routing decision	Forward the datagram
• Handles the information entry for remote network • Verify if the default network is configured • Perform the function to ensure network is reachable via best path to get to the network • Keep the possible multi path with equal-cost entry in the routing table • Perform the queuing process for the outgoing interface	• Handles the validation of the incoming frame with the correct Layer2 address • Characterize the frame and check frame if it passes CRC • Perform the stripping of the Layer2 header and trail from the frame, then check the destination address within cache entries • Creates the appropriate cache header and trailer needed for forwarding of the packets to outbound interface queue

Routers traffic forwarding

- For a router to forward traffic to the out-bound interface the routing table entry is important ensuring that the network topology is understood
  - Routing tables entries that contains the information's of the routes learned from other routers

Router switching functions



1. Accept and check the framing and buffer the packets to the memory
2. Determine the routing decision to where the datagram should be forwarded
3. Encapsulate the packets and forward the frame to the outbound interface

Process happens on Inbound interface of the router

Verifying the routing table entry to process the forwarding of the packets to the outbound interface

Process of forwarding the frame to the Outbound interface of the router for the destination network

Classful and classless distinction

Types of routing protocols

- Routing protocol are essentially application inside the router to designed to ensure correct and timely exchange of information within the network
- IP routing protocol has several distinctions which can be divided into different groups
  - The first is the group is on how the routing protocol handles the subnet mask sent during the routing update
  - The early routing protocol doesn't support this but the newer one's like (RIP2, OSPF, ISIS, BGP4) supports it, this distinction is called "classful and classless"

Classful routing protocol (obsolete)

- Periodic updates done by the routing protocol does not carry subnet or routing mask because the assumption is always based on network bit boundaries, and does not support VLSM which makes it inefficient for addressing the network
- This was obsolete for long time but for knowledge purposes there are two protocols design for it.
  - RIPv1
  - IGRP
- It has created constrains to the IP network design due to its limitations

Classless routing protocol

- Classless routing protocol was designed to overcome the constraint from classful which leads also to the development of RIP2 along with the routing protocols like:
  - OSPF
  - IS-IS
  - EIGRP (Cisco)
  - BGP

Characteristics of classless

- Support for different subnets mask value and can be configured with the routers to have different subnet mask (VLSM)
- The routes summarisation is now done in manual configuration, and provides Supports for Classless Interdomain Routing (CIDR) architecture

Distance Vector

Distance Vector routing protocol

- Another distinction is the Distance vector and Link-State protocols which differ from each other based on the behavior of learning the path to the destination network
- Distance vector routing protocol like RIPv2 are early technology of IP routing protocols and the concept of the designed was for small networks

Distance Vector operation

- Distance Vector maintains its own table by sending its own modified table for updates, sending updates to directly connected neighbors is done in a periodic manner. This is commonly known as the (routing by rumor)
- Updating of the tables affect the entire routing table except those networks learned from interfaces where update is sent, in the periodic update the timer needs to reach expiration stage before the next update will be sent.

Distance Vector techniques

- To prevent routing loops it employs the following:
  - Count to infinity conditions due to vanished routes
  - Split horizon
  - Poison reverse
  - Hold-down
  - Triggered updates

Link-state

Link-state routing protocol

- Link-state routing protocol was designed to overcome the limitation of Distance Vector routing protocol, the main goal is to achieved the following:
  - Maintain a loop-free and accurate table
  - Utilises multicast address and make updated based on incremental
  - Fast convergence of the network
  - Reduce the network overhead during updates
  - Selection of best path based on link status
- Routing protocol that supports link-state are:
  - OSPF
  - IS-IS

Link-state protocol timers

- OSPF
  - Incremental update is use when there is state change in the network
  - 30 minutes after the last update was received
- IS-IS
  - Incremental update is use when there is state change in the network
  - 15 minutes refresh interval after the last update
  - LSP periodical update to avoid remaining lifetime on the receiving router from reaching 0

Link-state operation

- Link state operates thru its main concern focusing on the link connected to the router (not the routes)
- During its operation if there is a change in the link state it will be propagated to its neighboring routers to maintain the same image of the network topology among each neighbors, and the resources used was the routers CPU instead of bandwidth like in the case Distance Vector
- When is identifies a problem the *incremental update* is sent to neighboring routers immediately, but remain silent if there's no change in the link state.

Link-state operation

- Maintains the topology map of the network for easy local network table updates via incremental updates
  - OSPF = Link State Advertisement (LSA)
  - Dijkstra algorithm to compute the new topology map of the network
- Metric used in Link state was stated as "*cost*" equipment vendors default value setting can be overridden in manual configuration

Link-State comparison chart

Characteristic	OSPF	IS-IS
Hierarchical topology	X	X
Retains knowledge of all possible routes	X	X
Routes summarisation - manual	X	X
Event-triggered announcement	X	X
Load balancing – equal path	X	X
VLSM support	X	X
Routing algorithm	Dijkstra	IS-IS
Metric	Cost	Cost
Hop Count limit	Unlimited	1024
Scalability	Large	Vry-Lrg

Interior and exterior routing protocols

- Other group distinction with routing protocol is the interior and exterior protocols which can be simplified as the protocol used for internal or external network
- Interior
  - Routing protocol use to maintain routes within the organisation
  - Routing protocol that support it are:
    - *RIPv2, OSPF, IS-IS, EIGRP (Cisco)*
- Exterior
  - Routing protocol use to maintain routes connecting to different organisation
  - Exchange routing information between organisation
    - Using Exterior Gateway Protocol (EGP)
  - Border Gateway Protocol version 4 (BGP-4)

Written exercise ☺

Please answer the attached worksheet material in your student manual

- Objective
  - To practice what you have learned

Written exercise 1

- Routing protocol comparison ☺

Summary

- After this module you should be able to perform the following:
  - List information's a router requires to route a data
  - Distinguish the difference between classful (obsolete) and classless
  - Differentiate Distance vector and Link-state protocol
  - Identify routes field within the routing table

Asia Pacific Network Information Centre

APNIC

Questions?

Asia Pacific Network Information Centre

APNIC

IP addressing

Asia Pacific Network Information Centre

APNIC

Overview

- IP addressing Issues and solution
- Variable Length Subnet Mask (VLSM)
- Written exercise : VLSM calculation
- Summarisation of routes
- Classless InterDomain routing (CIDR)
- Internet registry IP management procedure
- Written exercise : Route summarisation

Objectives

- To be able to perform the following tasks:
  - Use VLSM to extend the range of an IP address
  - Calculate proper distribution of IP addresses within your network to avoid wastage of addresses
  - Perform routes summarisation and be able to explain it

Addressing issues and solutions

IP addressing issues

- Exhaustion of IPv4 addresses
  - Wasted address space in traditional subnetting
  - Limited availability of /8 subnets address
- Internet routing table growth
  - Size of the routing table due to higher number prefix announcement
- Tremendous growth of the Internet

IP addressing solutions

- Solutions = Subnet masking and summarisation
  - Variable-length subnet mask definition
  - Hierarchical addressing
  - Classless InterDomain Routing (CIDR)
  - Routes summarisation (RFC 1518)
- Private address usage (RFC 1918)
- Network address translation (NAT)
- Development of IPv6 address

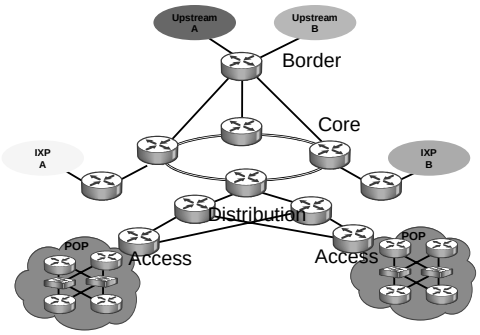
Subnetting overview

- It allows to create additional sub-networks by simply moving the network boundary to *right*
- When the contiguous *1s* is added it indicates by how many bits the network portion will be extended
- The sub-network is calculated by the 2^n where "*n*" is the number of extended bits.

Addressing Hierarchy

- Support for easy troubleshooting, upgrades and manageability of networks
- Performance optimisation
  - Scalable and more stable
  - Less network resources overhead (CPU, memory, buffers, bandwidth)
- Faster routing convergence

Addressing Hierarchy example



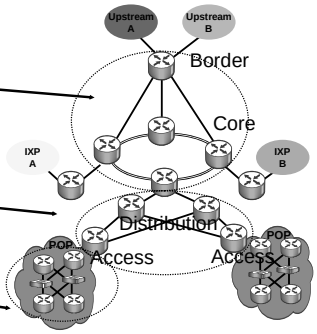
Addressing Hierarchical (cont.)

Network Number
192.168.0.0/16

Core
192.168.32.0/19

Distribution/Core
192.168.32.0/21

Access/Distribution
192.168.48.0/21

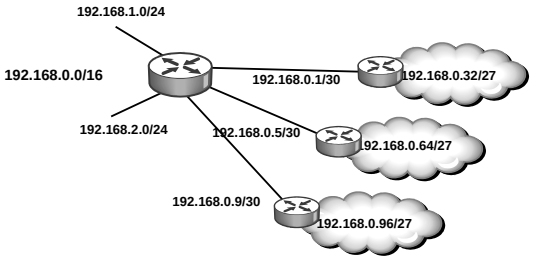


Variable Length Subnet Mask

- Allows the ability to have more than one subnet mask within a network
- Allows re-subnetting
  - to be able to create sub-subnet network address
- Increase the routes capability
  - Addressing hierarchy
  - Summarisation

Calculating VLSM example

- Subnet 192.168.0.0/24 into smaller subnet
  - Subnet mask with /27 and /30



IP addresses – IPv4

- IP addresses
  - An identifier for a computer & host/device on a network
- IPv4 (Internet Protocol version 4)
  - 32 bits numeric address written in 4 fields separated by dots

11001010 . **00001100** . **00011101** . **00000001**

(max value per field: 11111111)

or

202 . **12** . **29** . **1**

(max value per field: 255)

Decimal & binary

Decimal numbers *("base ten")*

2 3 5

$5 \times 10^0 = 5 \times 1 = 5$
$3 \times 10^1 = 3 \times 10 = 30$
$2 \times 10^2 = 2 \times 100 = 200$

235

0,1,2,3,4,5,6,7,8 & 9
(10 combinations)

Binary numbers *("base two")*

1 1 1 0 1 0 1 1

$1 \times 2^0 = 1 \times 1 = 1$
$1 \times 2^1 = 1 \times 2 = 2$
$0 \times 2^2 = 0 \times 1 = 0$
$1 \times 2^3 = 1 \times 8 = 8$
$0 \times 2^4 = 0 \times 16 = 0$
$1 \times 2^5 = 1 \times 32 = 32$
$1 \times 2^6 = 1 \times 64 = 64$
$1 \times 2^7 = 1 \times 128 = 128$

235

0 & 1
(2 combinations)

Binary to decimal conversion

1 1 1 1 1 1 1 1 =
$= 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$ =
= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

11001010.10111011.00010000.11111101 = ?

11001010 = 128+64+0+0+8+0+2+0 = 202
10111011 = 128+0+32+16+8+0+2+1 = 187
00010000 = 0+0+0+16+0+0+0+0 = 16
11111101 = 128+64+32+16+8+4+0+1 = 253

11001010.10111011.00010000.11111101

= 202.187.16.253

Decimal to binary conversion

7

7/2	→ 3	1
3/2	→ 1	1
1	→ →	1

→ 111

(check: 111 = 4+2+1 = **7**) *ok!*

95

95/2	→ 47	1
47/2	→ 23	1
23/2	→ 11	1
11/2	→ 5	1
5/2	→ 2	1
2/2	→ 1	0
1	→ →	1

→ 101111

(check: 101111 = 64+0+16+8+4+2+1 = **95**) *ok!*

202

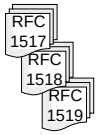
202/2	→ 101	0
101/2	→ 50	1
50/2	→ 25	0
25/2	→ 12	1
12/2	→ 6	0
6/2	→ 3	0
3/2	→ 1	1
1	→ →	1

→ 11001010

(check: 11001010 = 128+64+0+0+8+0+2+0 = **202**) *ok!*

Classful and classless

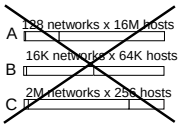
- Classful *(Obsolete)*
  - Wasteful address architecture
    - network boundaries are fixed at 8, 16 or 24 bits (class A, B, and C)
- **Classless** (Best Current Practice)
  - Efficient architecture
    - network boundaries may occur at any bit (e.g. /12, /16, /19, /24 etc)
- CIDR
    - Classless Inter Domain Routing architecture
  - Allows *aggregation* of routes within ISPs infrastructure



Classless & classful addressing

Best Current Practice

Classful



Obsolete
- *inefficient*
- *depletion of B space*
- *too many routes from C space*

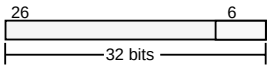
Classless

Addresses	Prefix	Classful	Net mask
...	...	...	...
8	/29		255.255.255.248
16	/28		255.255.255.240
32	/27		255.255.255.224
64	/26		255.255.255.192
128	/25		255.255.255.128
256	/24	1 C	255.255.255.0
...	...	...	...
4096	/20	16 Cs	255.255.240.0
8192	/19	32 Cs	255.255.224
16384	/18	64 Cs	255.255.192
32768	/17	128 Cs	255.255.128
65536	/16	1 B	255.255.0.0
...	...	...	... *

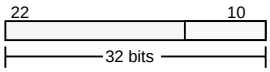
* See back of slide booklet for complete chart

- Network boundaries may occur at *any* bit

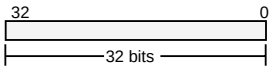
What is a slash?



→ 32 – 26 = 6 bits
→ /26 = 2^6 = 64



→ 32 – 22 = 10 bits
→ /22 = 2^{10} = 1024



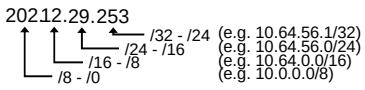
→ 32 – 32 = 0 bits
→ /32 = 2^0 = 1

/20 = $2^{(32-20)}$ = 2^{12} = 4096

/16 = $2^{(32-16)}$ = 2^{16} = 65 536

/0 = $2^{(32-0)}$ = 2^{32} = 4 294 967 296 (~ 4,3 Billion)

Ranges and slashes



10.0.0.0/25 → /25 = 128 addr = → 0 - 127 : 10.0.0.0 - 10.0.0.127

10.0.0.0/24 → /24 = 256 addr = → 0 - 255 : 10.0.0.0 - 10.0.0.255

10.0.0.0/23 → /23 = 2 */24s = → 0.0 - 1.255 : 10.0.0.0 - 10.0.1.255

10.0.0.0/20 → /20 = 16 */24s = → 0.0 - 15.255 : 10.0.0.0 - 10.0.15.255

10.0.0.0/13 → /13 = 8 */16s = → 0.0.0 - 7.255.255 : 10.0.0.0 - 10.7.255.255

Written exercise 2 ☺

Please answer the attached worksheet material in your student manual

- Objective
  - To practice what you have learned

Written exercise 2

- VLSM computation ☺

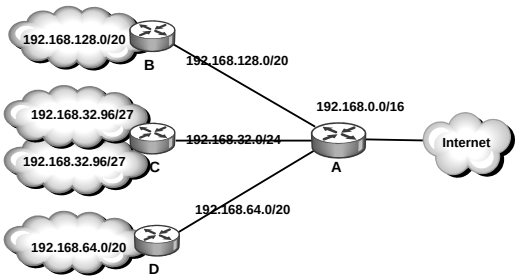
Summarisation of routes

Route summarisation

- Allows the presentation of a series of networks in a single summary address.
- Advantages of summarisation
  - Reducing the size of the routing table
  - Simplification
  - Hiding Network Changes
  - Network growth

Summarisation example

- Router C summarises its networks (2 x/27) before announcing to its neighbors (routers B and D)
- Router A combined the networks received from B, C, D and announce it as single /16 routing to Internet



Configuring summarisation

- Manual configuration is required with the use of newer routing protocols
  - Each of the routing protocols deal with it in a slightly different way
- All routing protocols employ some level of automatic summarisation depending on the routing protocol behavior (be cautious about it)

Manual summarisation

- Manual summarisation uses by OSPF are more sophisticated.
  - Sends the subnet mask including the routing update which allows the use of VLSM and summarisation
- Performs a a lookup to check the entire database and acts on the longest match

Discontiguous networks

- A network not using routing protocol that support VLSM creates problem
  - Router will not know where to send the traffic
  - Creates routing loop or duplication
- Summarisation is not advisable to network that are discontiguous
  - Turn off summarisation
    - Alternative solution but understand the scaling limitation
    - Find ways to re-address the network
  - Can create disastrous situation

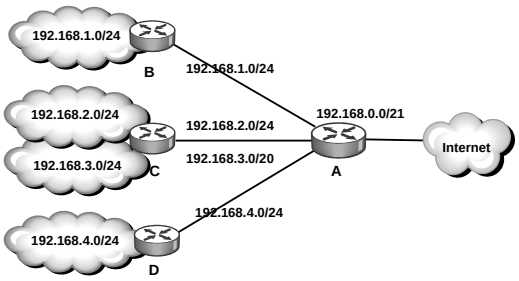
Classless Inter Domain Routing (CIDR)

Prefix routing / CIDR

- Prefix routing commonly known as classless inter domain routing (CIDR)
  - It allows prefix routing and summarisation with the routing tables of the Internet
- RFCs that talks about CIDR
  - *RFC 1517* Applicability statement for the implementation of CIDR
  - *RFC 1518* Architecture for IP address allocation with CIDR
  - *RFC 1519* CIDR : an address assignment and aggregation strategy
  - *RFC 1520* Exchanging routing information access provider boundaries in a CIDR environment

CIDR solution advantage

- CIDR offers the advantages reducing the routing table size of the network by summarising the ISP announcement in a single /21 advertisement



Internet Registry Procedures

IP Address Management

Revision of routing protocols

Interior Gateway Protocol (IGP)

- Examples are OSPF, EIGRP, ISIS
- Used to find optimum route to a host in ISP network
- Convergence becomes important with scaling

Border Gateway Protocol (BGP)

- Can be interior (iBGP) and exterior (eBGP)
- Used to carry traffic across your network and to/from the Internet
- Can use BGP attributes for routing policy

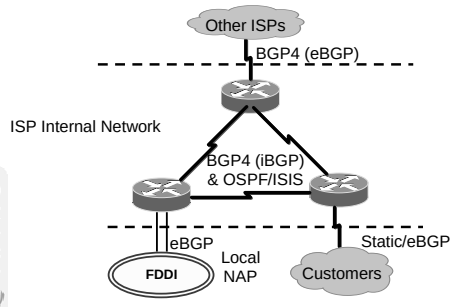
Principles of addressing

- Separate customer & infrastructure address pools
  - Manageability
    - Different personnel manage infrastructure and assignments to customers
  - Scalability
    - Easier renumbering - customers are difficult, infrastructure is relatively easy

Principles of addressing

- Further separate infrastructure
  - 'Static' infrastructure examples
    - RAS server address pools, CMTS
    - Virtual web and content hosting LANs
    - Anything where there is no dynamic route calculation
- Customer networks
  - Carry in iBGP , do not put in IGP
    - No need to aggregate address space carried in iBGP
    - Can carry in excess of 100K prefixes

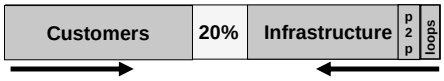
Hierarchy of routing protocols



IP Mgmt

Management - simple network

- First allocation from APNIC
  - Infrastructure is known, customers are not
  - 20% free is trigger for next request

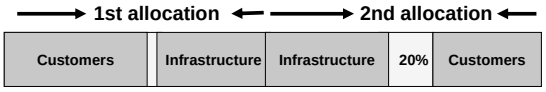


  - Grow usage of blocks from edges
  - Assign customers sequentially

IP Mgmt

Management - simple network

- If second allocation is contiguous

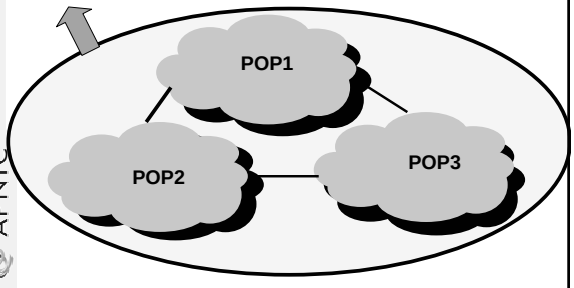


  - Reverse order of division of first block
  - Maximise contiguous space for infrastructure
    - Easier for debugging
  - Customer networks can be discontiguous

IP Mgmt

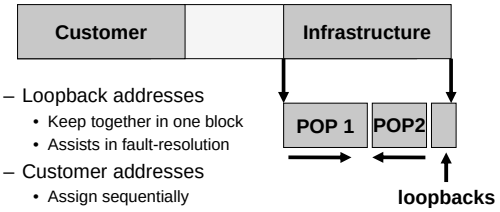
Management - many POPs

- WAN link to single transit ISP



Management - many POPs

- POP sizes
  - Choose address pool for each POP according to need



  - Loopback addresses
    - Keep together in one block
    - Assists in fault-resolution
  - Customer addresses
    - Assign sequentially

Management - many POPs

- /21 minimum allocation not enough for all your POPs?
  - Deploy addresses on infrastructure first
- Common mistake:
  - Reserving customer addresses on a per POP basis
- Do not constrain network plans due to lack of address space
  - Re-apply once address space has been used

Questions ?

Material available at: www.apnic.net/training/recent/

Written exercise 3 ☺

Please answer the attached worksheet material in your student manual

- Objective
  - To practice what you have learned

Written exercise 3

- Route summarisation ☺

Questions?

Network planning essentials

Overview

- Simple network plan
- ISP addressing plan
- Border router
- Core router
- Aggregation router
- Services router
- NOC router
- Access router
- Out-of-band console servers

Simple network plan

Hierarchical network design

- A network with different layers
  - Each level of the network has it own function
- Minimise costs
  - Avoid spending money to buy unnecessary feature of equipment to each layer requirements
  - Save bandwidth due to modularity of design
- Scalability is the major goal
  - Fast convergence
  - Route summarisation

Flat versus hierarchical network

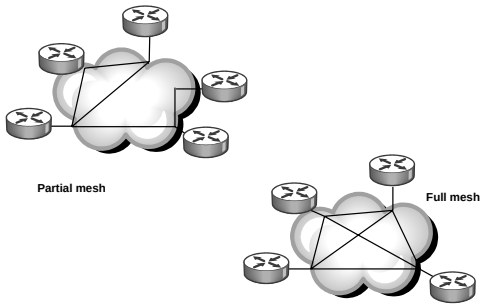
- Adequately designed for small network
  - Easy to design and maintain as long the network stays small
- No hierarchy
- All networking device have the same jobs
- No layer divisions

Mesh versus full-mesh topology

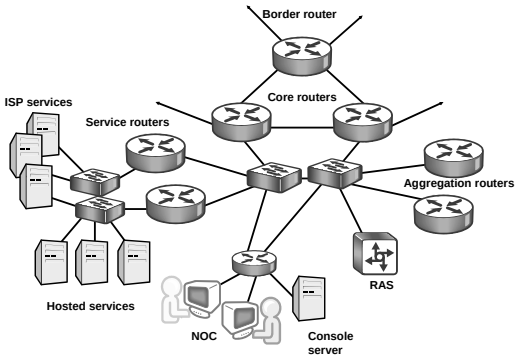
- Recommended by network designers is a mesh topology
- Good performance and provide redundancy
  - Partially mesh topology
    - Has fewer connections
    - Each router may require traversing from other intermediate link to go to other device
  - Full-mesh topology
    - All routers are connected to each other to offer good performance

Formula for full-mesh = (N x (N – 1))/2

Mesh versus full-mesh topology



Simple network plan



Border router

- Is the most important of the ISP network
- It provides connectivity to the rest of the Internet service providers in the world
- Protect the ISP network and the customers network from the Internet
- Its configuration is critical and should be correct because this is the main reason for the business connection

Core router

- Critical for connectivity it should be design to have a redundant component
- In configuration this router
  - Enable routing feature for optimised packet throughput
  - Avoid using filtering which will slow down manipulation of packets
  - Avoid usage of routing policy for filtering purposes
- Should be high-speed to switch packet easily and faster

Aggregation router

- Aggregation or gateway router for connecting fixed line customers
- Improve routing protocol performance
- Allows summarisation of routes from an aggregated address
- Allows configuration of routing policy for the customers network announcements

Services router

- Used for services provided to customers
  - DNS, email, news
  - Hosted services (content provided)
    - Web, email, DNS
- Configured by default to have filter to allow only the authorised users
- Routers with firewall features are often used there days or firewall itself
- Protect the core services provided by the ISP

NOC router

- Connects ISP essential services
  - Syslog, TACACS+, primary DNS
- Operations engineers network
  - Trouble isolations
  - Network monitoring
  - Research network testing
  - Staging area (option)

Access router

- Routers design to provide access services
  - Dial-up access
  - Cable services (on demand)
  - DSL on demand service
  - Wireless services (Wifi)
- All customers connecting to this network are required to provide proper authentication credentials

Out-of-band console server

- Can be typical router that has Async port configure for out-band access
- Allows remotes access of routers without using the in-band network
- Access to routers to its console port
- Utilise a different network
  - Not to be affected if the in-band network is down
  - Only small bandwidth usage is required

Questions?

Router configuration requirements

Overview

- Router overview
- Router configuration requirements
  - Security requirements
  - Monitoring options
  - Accessibility options
- Lab scenario: Configuring router initial requirements
- Summary

Router overview

What is a router?

- A device in the network that processes and routes data between two points
- A device that routes data between networks using IP addressing
- A layer 3 device
- Hardware or software used to connect two or more networks

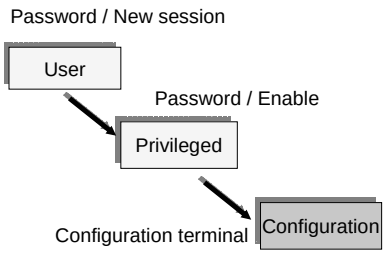
Router basics

- Operating systems
  - IOS (Cisco)
  - Free BSD base (Juniper)
- Several interfaces
  - Ethernet/Fast Ethernet, Serial, Gigabit port, Management port
- Management Interfaces
  - GUI based (web)
  - Command line interface (CLI)

Router components

ROM Bootstrap OS Rxboot	**Flash** OS Other files
NVRAM Startup configuration	**RAM** Active config Tables Buffers

Router modes

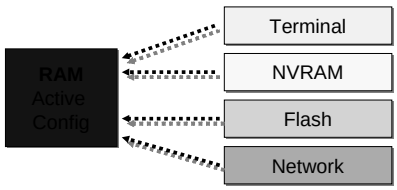


Router modes

- User mode
  - Check the router status and operation
  - Configuration is not visible
  - Prompt = ***router>***
- Privileged mode
  - Allows complete control to the router
  - Does not allow alteration of configuration
  - Prompt = **router#**
- Configuration mode
  - Mode to change configuration settings
  - Full control of the router configuration
  - Prompt = **router(config)#**

Router configuration mode

- Configuration
  - Active configuration
    - ***show running-config***
  - Startup configuration
    - ***show startup-config***



Router component

Read Only Memory (ROM) chips

- ROM Monitor (bootstrap program)
  - Firmware that runs when the router is boot up or reset
- Certain task can be done using the ROM monitor
  - Password recovery option
  - Downloading the software image using the management port
- Runs if there are no software images available on the router (with early model routers)

Router component

Flash Memory

- Stores the software image of the router
- Usually built into the router
- Some vendors also provide external flash memory card or disk

- Allows update of router software image with less interruption of service
  - Image can be upgraded without affecting the existing image running in the router
  - Install the software then instruct the router to boot the new image after the next boot
- Allows the router to load other information
  - Router logs
    - Crash information of the router
    - Debug information

Router component

Non-Volatile RAM (NVRAM)

- Stores the existing running configuration
- Router start-up boot configuration

- Tiny memory size
- Stored configuration is very important
  - Upon router reboot / shutdown
  - Because RAM information is lost during reboot and shutdown

Router component

Random Access Memory (RAM)

- Stores the current working configuration
- Handles the tables and buffers
- Non-permanent memory

- Broken down into two main areas
  - Main processor memory
    - Stores entry for the routing table, ARP table, and current running configuration
  - Shared processor memory
    - Buffer location for temporary stored packets for process

Router configuration

Router configuration requirements

- In configuring router we need to address the following requirements.
  - Security
  - Manageability
  - Accessibility

Router security requirements

Security requirements

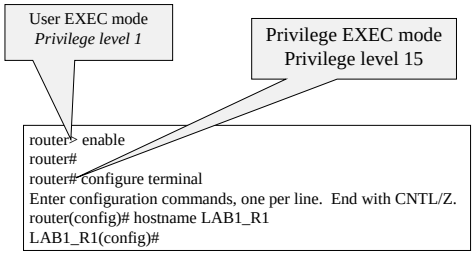
- To secure the router, the setup should enable the following:
  - Provide names to your router
  - Banner information
  - Configure password for the router
  - Access with privilege per user
  - Authentication and Authorisation
    - Locally configured
    - Remote server access (TACACS/RADIUS)
  - Access filters policy
  - Enable logging for auditing
  - Disable unnecessary services running

Reminders

- All configuration samples are Cisco based configuration

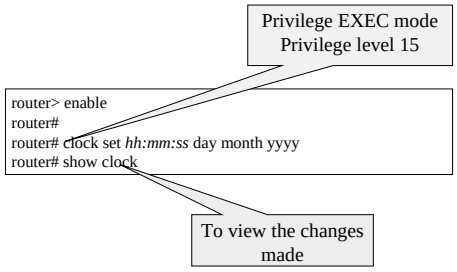
Security requirements

Provide Hostname for your router



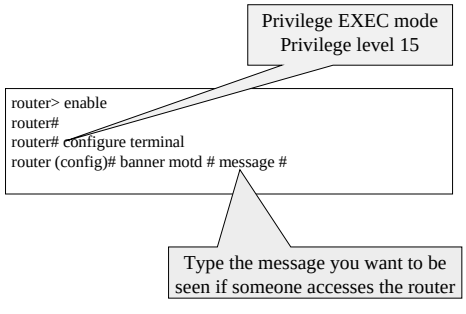
Security requirements

Setting the clock manually



Security requirements

Setting the Banner



Security requirements

Setting the password

Enable password

For global configuration command Cisco method

```
router> enable
router#
router# configure terminal
router (config)# enable password test
```

Secret password (with MD5)

```
router> enable
router#
router# configure terminal
router (config)# enable secret testing1
```


Security requirements

Setting the password

Line console password

For console access password (if accessing via console)

```
router> enable
router#
router# configure terminal
router (config)# line console 0
router (config)# password test
```

Virtual terminal lines password (vty)

For vty access password (if access is via telnet)

```
router> enable
router#
router# configure terminal
router (config)# line vty 0 4
router (config)# password test
```


Security requirements

- Access privilege
  - Allow users to view only the router stats
  - Non-administrative command (not allowed to change any config)

```
Router - 12.0.5.T and Later
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server privilege exec level 7 ping
privilege exec level 7 configure terminal privilege exec level 7 configure
```

Security requirements

With Cisco routers there are three privilege levels by default.

- **Privilege level 1** = non-privileged (prompt is router>), the default level for logging in
- **Privilege level 15** = privileged (prompt is router#), the level after going into enable mode
- **Privilege level 0** = seldom used, but includes 5 commands: ***disable***, ***enable***, ***exit***, ***help***, and ***logout***
- **Levels 2-14** are not used in a default configuration, but commands that are normally at level 15 can be moved down to one of those levels and commands that are normally at level 1 can be moved up to one of those levels. Obviously, this security model involves some administration on the router.

Cisco Systems Tech Notes

Sample configuration

Cisco router configuration

Router - 12.0.5.T and Later
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server privilege exec level 7 ping
privilege exec level 7 configure terminal privilege exec level 7 configure

Cisco Systems Tech Notes

Sample configuration

Server configurations

Follow these steps to configure the server.

- Fill in the username and password.
- In Group Settings, make sure shell/exec is checked, and that 7 has been entered in the privilege level box.

TACACS+ - Stanza in Freeware Server

Stanza in TACACS+ freeware:
user = seven { login = cleartext seven
service = exec { priv-lvl = 7
}
}

Cisco Secure UNIX TACACS+
user = seven
{ password = clear "seven"
service = shell { set priv-lvl = 7
}
}

Cisco Systems Tech Notes

Sample configuration

Access policy filters for telnet users

Access list filters for telnet user allowing only the IP written

```
access-list 103 remark VTY Telnet Access ACL
access-list 103 permit tcp host <IP address> host x.x.x.x eq 23 log-input
access-list 103 permit tcp host <IP address> host x.x.x.x eq 23 log-input
access-list 103 deny ip any any log-input
```

```
line vty 0 4
access-class 103 in
exec-timeout 15 0
transport input telnet
```

Enabling the filters on the router line vty 0 4

Sample configuration

Access policy filters for telnet and SSH users

Access list filters for telnet and SSH user allowing only the IP written

```
access-list 104 remark VTY Telnet and SSH Access ACL
access-list 104 permit tcp host <IP address> host x.x.x.x range 22 23 log-input
access-list 104 permit tcp host <IP address> host x.x.x.x range 22 23 log-input
access-list 104 deny ip any any log-input
```

```
line vty 0 4
access-class 104 in
exec-timeout 15 0
transport input telnet ssh
```

Enabling the filters on the router line vty 0 4 for telnet and SSH users

Sample configuration

Enabling logging for auditing

Configure log time stamps, logging size, timezone for proper time, source interface of the log messages for the log server

```
service timestamps debug datetime msec show-timezone localtime
service timestamps log datetime msec show-timezone localtime
logging buffered 16384 debugging
no logging console
clock timezone GMT 0

int loopback0
ip address 10.192.168.X 255.255.255.255
no ip redirects
no ip unreachables
no ip proxy-arp
no ip directed-broadcast
```

Sample configuration

Enabling logging for auditing (cont)

```
logging trap debugging
logging facility local5
logging source-interface loopback0
logging <IP Address of syslog server>
```

Set the logging facility to be captured by the syslog server, identify the source interface of logs, provide the syslog server address

Disable unused access and services

- Disable http servers running if not in use
  - http and secure http server
- Disable discovery protocol
  - CDP (Cisco)
- Disable services which can be used for reconnaissance attempts
  - Ip soure-route, finger, boot server, domain-lookup, service pad

Router manageability requirements

Manageability requirements

- Be able to monitor the router's performance
  - Interfaces
  - CPU

Enable SNMP for monitoring purposes

- Allow only specific host
- Enable the use of READ-ONLY access
- Protect with difficult password

Sample configuration

Enabling SNMP for monitoring

Configure with SNMP access filter by allowing only the server host address that can query the router

```
access-list 20 remark SNMP ACL
access-list 20 permit <IP Address of SNMP server>
access-list 20 deny any log
```

```
snmp-server community <COMMUNITY> RO 20
```

configure the community to allow READ-ONLY access from the host included in the filters

Router accessibility requirements

Accessibility requirements

- Be able to manage the routers properly
  - Enable console and VTY line to
    - Allow access to the router
      - With specific host only (using filters)
    - Enable the use of privileges access
  - Provide the use of out-of-band management
  - Setup a centralised management console to control all devices

Lab exercise 1 ☺

Please perform the required configuration in the attached worksheet material in the student manual

- Objective
  - To practice what you have learned

Lab exercise 1

- Configuring initial requirements ☺

Questions?

Configuring OSPF in a single area

Overview

- Objectives
- Terminologies
- Different topology
  - Broadcast multi-access topology
  - Point-to-point topology
  - NBMA topology
- Written exercise: OSPF operation
- Configuring OSPF in a single area
- Verifying OSPF operation
- Lab scenario: Configuring OSPF in a single area

Objectives

- To understand how the OSPF protocol works
- To be able to configure a router running OSPF protocol
- To be able to verify the operation of OSPF inside the network with different topology scenarios

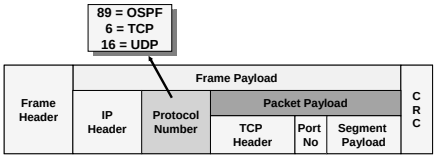
OSPF overview

Open Shortest Path First (OSPF)

- Open standard link state routing protocol (RFC 1247, 2328)
- Allows fast convergence of routes
- Supports VLSM
- Selects the path based on bandwidth
- Supports equal-cost multi-path

OSPF IP packet

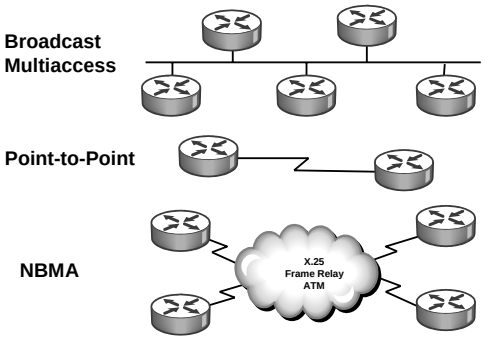
- To deliver routing information to neighboring router OSPF relies on IP packets and uses protocol port 89



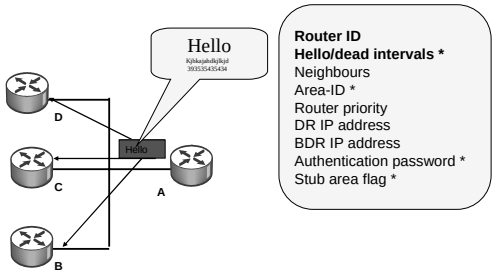
Terminology

- Autonomous systems
- Area
- Cost
- Neighbors database
- Topology database
- Routing table

Topologies

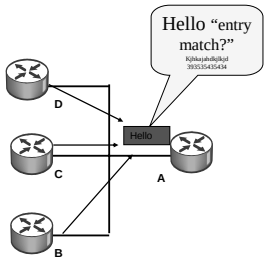


Neighbouring routers



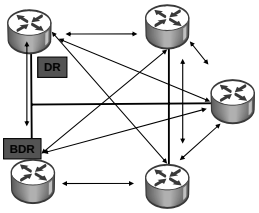
Router ID
Hello/dead intervals *
Neighbours
Area-ID *
Router priority
DR IP address
BDR IP address
Authentication password *
Stub area flag *

Neighbouring router (cont.)



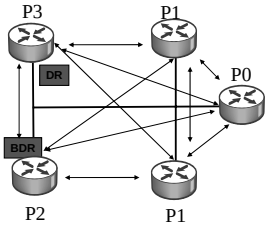
Router ID
Hello/dead intervals *
Neighbours
Area-ID *
Router priority
DR IP address
BDR IP address
Authentication password *
Stub area flag *

DR and BDR concept



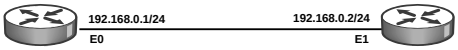
- Concept of DR and BDR was introduce to provide representation of segment and to manage updates efficiently
- Adjacency with the segment is formed with DR and BDR

Election of DR and BDR



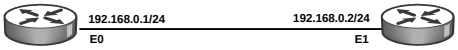
- Packets "Hello" is exchanged via IP multicast
- Highest priority is selected as DR by OSPF
- Highest priority elected

OSPF state process



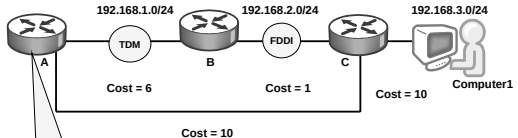
OSPF State							
Process	Down	Init	2-way	Ex-start	Exchange	Loading	Full
Hello! I am router ID 192.168.0.1 I don't see anyone →		Hello! I am router ID 192.168.0.2 and I see you →	Hello! I am router ID 192.168.0.1 I can see you now →				
Hello! Since I have ID 192.168.0.1 I will start the exchange →				Hello! Hey my ID is higher I will start the exchange →			
					Hello! Here is my LS database summary →		

OSPF state process (cont.)



OSPF State							
Process	Down	Init	2-way	Ex-start	Exchange	Loading	Full
Hello! Since I have ID 192.168.0.1 I will start the exchange →				Hello! Hey my ID is higher I will start the exchange →			
Hello! OK here is my LS database summary too →					Hello! Here is my LS database summary →		
Hello! OK LS Acknowledge give me your complete network statement →						Hello! Thanks LS acknowledge Here it is →	
Hello! OK LS Acknowledge thanks →							

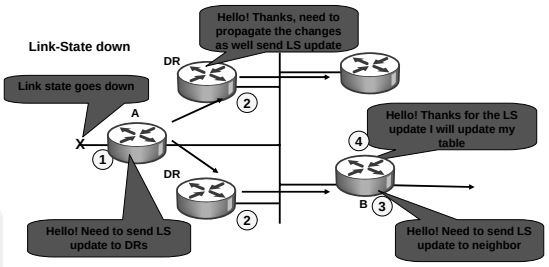
Shortest path route selection



Hello! According to topology table after processing the algorithm the best path is via 192.168.3.0 I prefer highest cost to reach Computer1

Topology Table		
NET	Cost	Out Interface
192.168.2.0	7	To0
192.168.3.0	17	To0
192.168.3.0	20	E0

Maintaining information

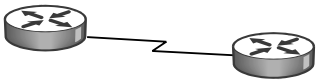


- Notifies DRs via multicast address 224.0.0.6
- DR then notifies others (neighbors) via multicast address 224.0.0.5

Maintaining information (cont)

- Check LSD entry → Same sequence number? "ignore"
- Add entry to LSD ↔ If higher update LSD
  → NO, send LSU with new information
- Send LSA to DR
- Flood LSA to neighbors
- Run SPF for the new routing table entry

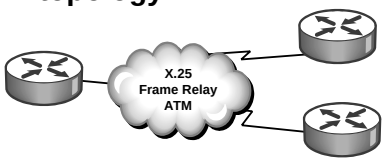
Point-to-Point scenario



- Router send "hello" to detects its neighbors
- The concept of DR and BDR is not followed, adjacency is automatic
- Just like broadcast networks the OSPF packets still uses multicast address 244.0.0.5

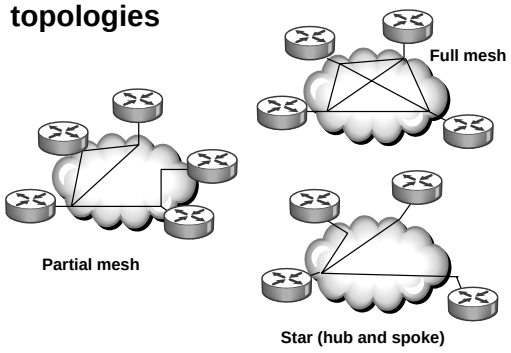
OSPF with NBMA topology

NBMA topology



- Non-broadcast Multi Access (NBMA) topology allows a single router interface to interconnect multiple routers
- Although NBMA supports interconnection of multiple routers it has no broadcast capability

NBMA = Frame-relay / ATM topologies



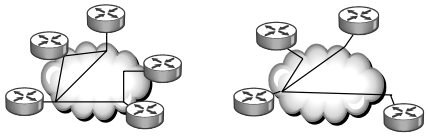
NBMA = Frame-relay / ATM topologies (cont.)

- In a typical NMBA topology sub-interface is used to interconnect routers
  - The interface is split into several sub-interface of normally called logical interfaces originating from a single physical interface.
  - Sub-interface support multiple, point-to-point or point-to-multipoint connections

DR and BDR selection in NBMA

- NBMA topology in the selection of DR is considered like other broadcast media however requires the following:
  - Full connectivity is required to perform the election of DR and BDR between all other routers in the NBMA topology
  - Neighbors must be listed and configured manually

Point-to-Multipoint mode



Partial mesh

Star (hub and spoke)

- Start topology and partial-mesh is the usual topology for point-multipoint
- The concept of DR/BDR election was not use in this topology and there is no requirements for static configuration for each neighbors

Written exercise 4 ☺

Please answer the attached worksheet material in your student manual

- Objective
  - To practice what you have learned

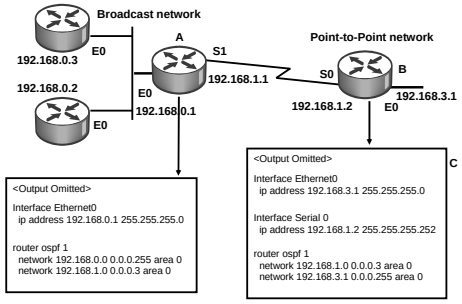
Written exercise 4

- OSPF operation in a single area☺

Configuring OSPF in a Single Area

Note: all configuration example commands are Cisco base

OSPF with internal routers



Optional commands


```
<Output Omitted>

Interface loopback0
 ip address 192.168.1.1 255.255.255.255

Interface Ethernet0
 ip address 192.168.0.1 255.255.255.0

router ospf 1
 router ID 192.168.1.1
 network 192.168.0.0 0.0.0.255 area 0
 network 192.168.1.1 0.0.0.0 area 0
```

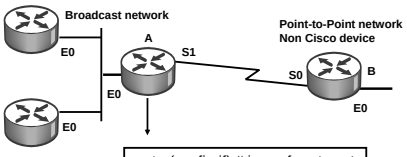
Router ID:

- **Router active interface IP address containing the highest IP address**

Loopback interface:

- **Highest IP address in the interface can be overridden by the loopback interface IP address and if several loopback interface is configured the highest IP address of any active loopback interface is used**

Optional commands cont.




```
router(config-if) # ip ospf cost cost
```

- Cost OSPF command is normally configured to the router outgoing interface connecting to non-Cisco devices to allow inter-operability

OSPF over NBMA topology

- NBMA mode configuration command
  router(config-if)#
  – **ip ospf network non-broadcast**

- Point-to-multipoint mode command
  router(config-if)#
  – **ip ospf network point-to-multipoint** [non-broadcast]

OSPF over NBMA topology (cont.)

- NBMA broadcast mode command

  router(config-if)#
  – **ip ospf network broadcast**

- Point-to-point mode command

  router(config-if)#
  – **ip ospf network point-to-point**

OSPF in NBMA mode

- Non-broadcast mode default, it needs the ***ip ospf network*** command
  – **ip ospf network broadcast**
- Neighbour statement is required
  – **neighbor ip-address [priority number] [poll-interval sec] [cost number]**

```
R1(config)# interface serial 0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# encapsulation frame-relay
R1(config-if)# ip ospf network non-broadcast
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.255. area 0
R1(config-router)# neighbor 10.1.1.2
R1(config-router)# neighbor 10.1.1.3
R1(config-router)# neighbor 10.1.1.4
```

OSPF in Point-to-Multipoint mode

- Point-to-Multipoint is normally used in a star topology and each connection is treated just like point-to-point and no election of DR/BDR election is taking place

```
R1(config)# interface serial 0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# encapsulation frame-relay
R1(config-if)# ip ospf network point-to-multipoint
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.255. area 0
```

OSPF in Broadcast mode

- In NMBA broadcast mode a full mesh topology is required for the automatic DR/BDR election or manual election can also be done based on priority

```
R1(config)# interface serial 0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# encapsulation frame-relay
R1(config-if)# ip ospf network broadcast
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.255. area 0
```

OSPF in Point-to-Point mode

- Sub-interface in the NBMA mode is treated as a physical point-to-point network by OSPF and the adjacency for such connection is automatic

```
R1(config)# interface serial 0
R1(config-if)# no ip address
R1(config-if)# encapsulation frame-relay
R1(config)# interface serial0.1 point-to-point
R1(config-subif)# ip address 10.1.1.1 255.255.255.0
R1(config-subif)# frame-relay enterface-dlci 51
R1(config)# interface serial0.2 point-to-point
R1(config-subif)# ip address 10.1.2.1 255.255.255.0
R1(config-subif)# frame-relay enterface-dlci 52
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.255. area 0
```

Verifying OSPF Operation

Note: all example verification commands are Cisco base

Verifying OSPF operation

- Verifying if OSPF is configure
  router#
  – **show ip protocol**
- Verifying all routes learned by the router
  router#
  – **show ip route**
- Verifying area ID adjacency
  router#
  – **show ip ospf interface**

Verifying OSPF operation (cont.)

- Verifying OSPF timers and statistics
  router#
  – **show ip ospf**
- Verifying information about DR, DBR and neighbors
  router#
  – **show ip ospf neighbor detail**
- Verifying link-state database
  router#
  – **show ip ospf database**

Verifying OSPF operation (cont.)

- Clearing the IP routing table entry
  router#
  – **clear ip route**
- Displaying debug outputs from the router
  router#
  – **debug ip ospf *option***

Lab exercise 2 ☺

Please perform the required configuration in the worksheet material of your student manual

- Objective
  - To practice what you have learned

Lab exercise 2

- Configuring OSPF in a single area ☺

Questions?

Basic BGP

Overview

- BGP overview
  - When to use BGP?
- BGP terminology
- BGP operation
- Written exercise: BGP terminology and operation
- Configuring BGP
- Lab scenario: BGP peering

Objectives

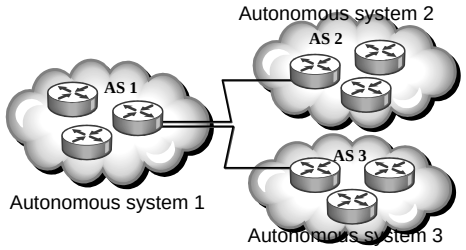
- To understand BGP protocol functions
- Describe how to connect an AS
- To be able to configure a router running BGP protocol
- To able to verify the operation of BGP inside the network

BGP overview

Autonomous systems

- An autonomous system (AS) is a collection of networks controlled by a common or single administrator
- Autonomous systems operate using:
  - Interior Gateway Protocol (IGP)
    - RIPv2, EIGRP, OSPF, ISIS
  - Exterior Gateway Protocol (EGP)
    - BGP verision 4 (RFC 1771)

Autonomous systems



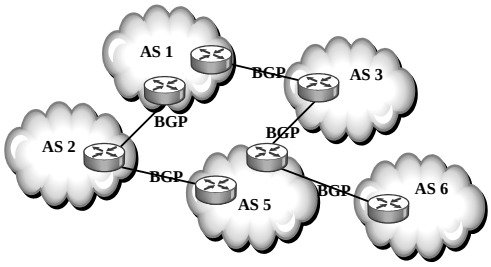
The connection protocol used within an AS (IGP) can be RIPv2, EIGRP, OSPF, or ISIS

BGP is used for the interconnection of different ASes (EGP)

Border Gateway Protocol (BGP)

- Inter-domain routing protocol
- BGP Version 4 (BGP-4)
- RFC 1771
- Used to connect different organisations using an Autonomous System Number (ASN)
- There are two types of ASN
  - Private
    - 64512 - 65535
  - Public
    - Issued by the internet registries
      - APNIC, ARIN, RIPE NCC, LACNIC, AFriNIC

BGP in between Autonomous systems



- BGP is used to interconnect ASes
- This guarantees loop-free routing information

When to use BGP

- BGP is the most appropriate application is for the following conditions:
  - An AS has multiple connections to different ASes
  - Packets are transmitted (transit) between third party ASes (as in an ISP scenario)
  - Decision is needed to control the traffic flow entering and leaving an AS
  - Route summarisation and aggregation of announcement exchanges from ASes

When BGP is not needed?

- BGP is not appropriate for the following conditions:
  - The AS only has single connection to the Internet or a different AS (upstream provider)
  - Routing policy is not the main concern to control the traffic flow to/from an AS

  With other conditions:

  - Router has limited memory and processing power
    - Can run BGP with partial or default route configuration
    - If full routes are required and transit is provided, may require higher capacity router to accommodate full routes or customer transit traffic
  - Low bandwidth between AS
    - Can run even with 64Kpbs link but with minimum configuration only (partial or default route only)

  Make use of static routes ☺

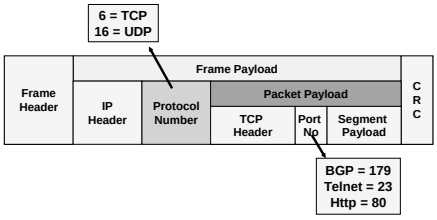
BGP terminology

Characteristics of BGP

- BGP is a path vector protocol
  - TCP port 179
  - PVP is UDP protocol 17
  - Incremental and triggered updates only
  - TCP connectivity is verified using periodic keepalives
  - Designed for large scale networks

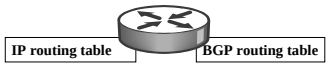
BGP packets

- Since BGP run on top of TCP port 179 it relies on TCP protocol for the reliability of the session



The tables

- If BGP is configured and running is creates its own table (BGP routing table) in addition to the existing IP routing table of the router (static route, IGP routes)
- However, both sets of information can be exchanged between the two tables (IP and BGP table)




```
P2R2#sh ip route

Gateway of last resort is not set

     192.168.2.0/28 is subnetted, 4 subnets
C       192.168.2.16 is directly connected, Loopback0
C       192.168.2.32 is directly connected, Serial0/0
C       192.168.2.48 is directly connected, FastEthernet0/0
```

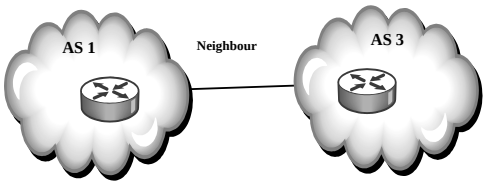
```
P2R2#sh ip bgp

BGP table version is 8, local router ID is 192.168.2.49
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.2.0/28   192.168.2.33             1             0 i
*  192.168.2.32/28  192.168.2.33             1             0 i
*> 10.100.100.0/24  192.168.2.33             1             0 i
*> 192.168.2.16/28  0.0.0.0                  0         32768 i
*> 192.168.2.32/28  0.0.0.0                  0         32768 i
*> 192.168.2.48/28  0.0.0.0                  0         32768 i
```

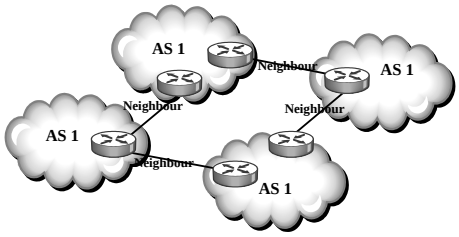
Peers = neighbours

- Two or more ASes exchanging BGP information are called peers or neighbours



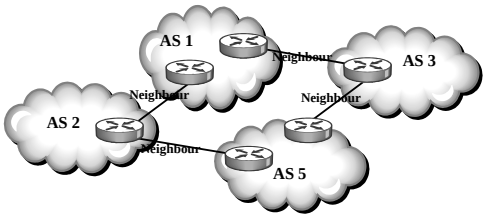
Internal BGP (iBGP)

- Neighbours that belong to the same AS can use internal BGP (iBGP)
- Note that these neighbours don't need to be directly connected



External BGP (eBGP)

- Neighbours that belong to different AS use external BGP (eBGP)
- Note that these neighbours need to be directly connected



Policy routing with BGP

- BGP supports the definition of policies or rules to manipulate the flow of data through the AS, and the rules is based on hop-by-hop routing
- However, some policies which are not supported by hop-to-hop may require using different techniques
  - For example source routing

BGP attributes

- The metrics used by BGP are called path attributes
- Two types of attributes
  - Well-know
  - Optional

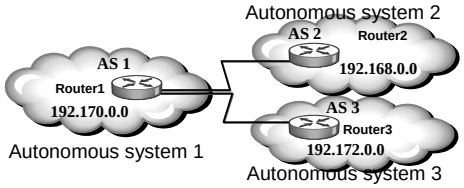
• Well-know	• Optional
– Mandatory – Discretionary	– Transitive – Nontransitive

BGP attributes (cont.)

- Well-know mandatory
  - AS-Path
  - Next-hop
  - Origin
- Well-know discretionary
  - Local preference
- Optional transitive
  - Community
- Optional nontransitive
  - Multi-exit-discriminator (MED)

AS-path attribute

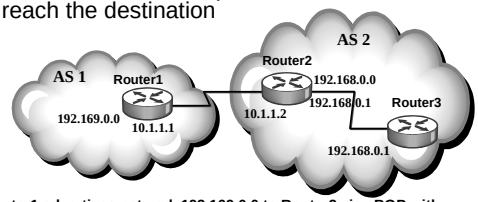
- Presents the list of ASes that a route has traversed in order to reach its destination



Router2 to needs to go to network 192.172.0.0
The AS-path passes through AS1 to AS3
AS-path to the network destination is AS1 and AS3 from AS2

Next-hop attribute

- Indicates the next-hop IP address used to reach the destination



Router1 advertises network 192.169.0.0 to Router2 via eBGP with next-hop 10.1.1.1 (Router 2 serial address)

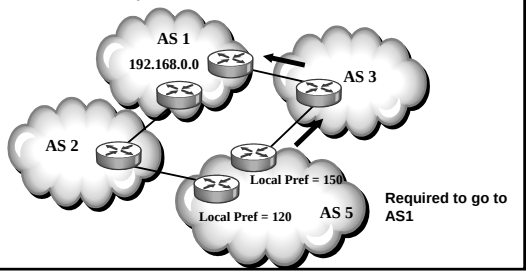
Router2 then advertises 192.169.0.0 via iBGP to Router3, and keeps the next-hop address 10.1.1.1 as the next-hop for the network 192.169.0.0

Origin attribute

- A well-known mandatory attribute that defines the path origin
  - The (i) for IGP if achieved by the *network* command in BGP
  - The (e) EGP which was coming from the redistribution made from EGP
  - The (?) is the incomplete mark for redistributed network from IGP or static

Local preference attribute

- Provides indication to router which AS path is preferred to exit the AS
  - Highest value is preferred once configured with routers running BGP
  - Allowed only for routers within the same AS

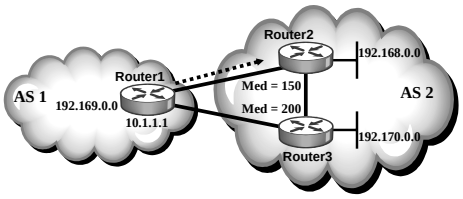


Community attribute

- Is an optional transitive attributes used for tagging of routes to ensure consistency on filtering and route-selection policy
- Tagging of routes can be made for the incoming and outgoing routing updates in the following purposes
  - Filtering of incoming routes
  - Outgoing routes updates from internal network or customer networks being announced
- Communities are dropped by default if the router does not understand it

MED attribute

- Lowest value is preferred if configured with BGP
- Used with routers connecting to external BGP peers only

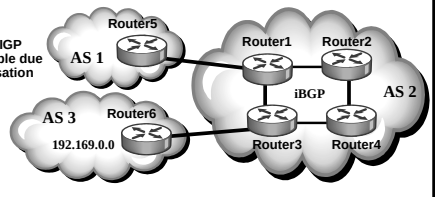


BGP synchronisation rules

- Routers cannot use or advertise any routes learned via iBGP to an external neighbour, until a route match is learned via IGP.
  - Ensuring route consistency throughout the AS but safer to turn off because it can cause problem sometimes

BGP synchronisation example

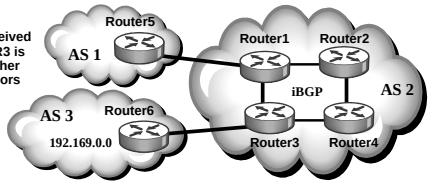
No matching IGP routes available due to synchronisation enabled



Example network with BGP synchronisation ON (default)

Router1, Router2, and Router4 would not use or advertise the route 192.169.0.0 until they receive the matching route via IGP which will keep Router 5 from not hearing anything about the network due to non-availability of routes in the IGP.

BGP synchronisation example



Example network with BGP synchronisation OFF

Router1, Router2, and Router4 would use and advertise the route they receive via iBGP from Router 3 and will allow announcement to Router5 so that Router 5 can hear about 192.169.0.0

Questions?

Basic BGP

Overview

- BGP overview
  - When to use BGP?
- BGP terminology
- BGP operation
- Written exercise: BGP terminology and operation
- Configuring BGP
- Lab scenario: BGP peering

BGP operation

BGP messages

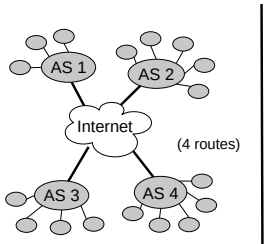
- BGP messages types are very important to understand to make sure that BGP is perfectly running
- Understanding the messages types will make it more easier to troubleshoot BGP problem
  - The “Open” message type contains the hold timer for BGP including the BGP router ID
  - The “Keepalive” is used for hold timer expiration
  - The “Update” handles the information for BGP updates but single path only
  - The “Notification” is for error detection to triggers the BGP protocol to close immediately if needed

Route selection decision

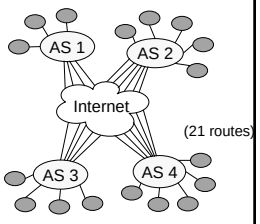
- The stages for the process selection of route decisions below is based on the assumption that routes are synchronised and no AS loops and valid next-hop:
  - Prefer highest weight (local to router)
  - Prefer highest local preference (within the AS)
  - Prefer routes originated by the local router
  - Prefer shortest AS-path
  - Prefer lowest origin code (IGP < EGP < incomplete)
  - Prefer lowest MED (from other AS)
  - Prefer eBGP path over iBGP path
  - Prefer the path through the closest IGP neighbor
  - Prefer oldest route for eBGP paths
  - Prefer the path with the lowest neighbor BGP routes ID
  - Prefer the path with the lowest neighbor IP address

Aggregated address

- Routes can be aggregated when sending announcement to ASes



(Aggregated announcement)



(No aggregation)

Written exercise 6 ☺

Please answer the attached worksheet material in your student manual

- Objective
  - To practice what you have learned

Written exercise 6

- BGP terminology and operations ☺

Configuring BGP

Note: all example commands are Cisco base

BGP configuration commands

- Starting the BGP routing process

  router bgp *autonomous-system-number*

- Defining the network to advertise

  network *network-number* ***mask*** *network-mask*

BGP configuration commands

- Setting the neighbour individually

  neighbor *ip-addresss* ***remote-as*** *autonomous-system-number*

- Setting the neighbours and defining peer groups

  neighbor *ip-addresss* | *peer-group-name* ***remote-as*** *autonomous-system-number*

BGP configuration commands

- Forcing the next-hop address

  neighbor *ip-addresss | peer-group* ***next-hop-self***

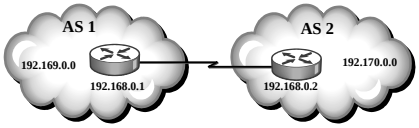
- Disabling synchronisation

  no synchronisation

- Summarising or aggregating routes

  aggregate-address *ip-addresss mask* ***[summary-only]*** *[**as-set**]*

BGP configuration sample



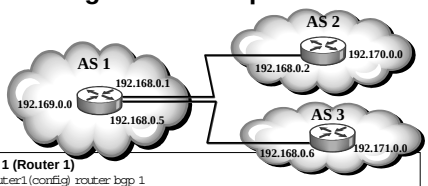
AS 1 (Router 1)

```
Router1(config) router bgp 1
Router1(config-router) neighbor 192.168.0.2 remote-as 2
Router1(config-router) network 192.169.0.0
```

AS 2 (Router 2)

```
Router2(config) router bgp 2
Router2(config-router) neighbor 192.168.0.1 remote-as 1
Router2(config-router) network 192.170.0.0
```

BGP configuration sample



AS 1 (Router 1)

```
Router1(config) router bgp 1
Router1(config-router) neighbor 192.168.0.2 remote-as 2
Router1(config-router) neighbor 192.168.0.6 remote-as 3
Router1(config-router) network 192.169.0.0
```

AS 2 (Router 2)

```
Router2(config) router bgp 2
Router2(config-router) neighbor 192.168.0.1 remote-as 1
Router2(config-router) network 192.170.0.0
```

AS 3 (Router 3)

```
Router3(config) router bgp 3
Router3(config-router) neighbor 192.168.0.5 remote-as 1
Router3(config-router) network 192.171.0.0
```

Managing and verifying BGP

- To ba able to manage and verify the BGP session running the following commands can be used:
  - Reset or route refresh for the BGP session to a neighbour

    clear ip bgp {***** | *ip-address}* [*soft* [***in*** | ***out***]]
  - Commands to view the BGP sessions informative

```
show ip bgp
show ip bgp paths
show ip bgp summary
show ip bgp neighbors
```

Lab exercise 4 ☺

Please perform the required configuration in the worksheet material of your student manual

- Objective
  - To practice what you have learned

Lab exercise 4

- Configuring BGP peering ☺

Questions?

Summary

Meet the course objectives

- Gain the appropriate foundation knowledge and be able perform the following:
  - Identify and differentiate routing protocols (RIP/OSPF/ISIS/BGP)
  - Simplify and manage addressing calculation effectively
  - Define each network layer to attain hierarchical addressing and correct protocol usage

Course objectives (cont.)

- Configure and perform initial router configuration requirements
- Configure OSPF in a single area and interconnect multi-area OSPF network
- Build and network running both OSPF and BGP protocol

Course topics discussed

- Building a start-up network with focus on configuring the following:
  - TCP/IP protocols and IP addresses
  - VLSM and route summarisation
  - OSPF and BGP protocol
  - Route announcements
  - Router interfaces configuration
  - Peering connection within and outside the network

Course contents

- Routing principles
- IP addressing
- Network planning essentials
- Router configuration requirements
- Configuring OSPF in a single area
- Configuring BGP

Thank you very much