AFIX Technical Workshop: Session 3

Technical Refresher

Terminology you will need for this session

You may find it useful to review the concept definitions below to refresh your existing networking knowledge. If you are thoroughly familiar with all these concepts, please feel free to skip directly to Section 2: Introduction to Routing.

Logical Network

A diagram or description of a network that is concerned only with connection paths and is independent of the physical location of each piece of equipment in the network.

Network layer

The Open Systems Interconnect (OSI) Reference model is an industry standard model for a layered networking architecture, in which each layer is responsible for a different part of the networking process.

The OSI model has seven layers:

Layer 7: Application

The level at which applications access the network services that directly support applications such as software for file transfers, database access, and electronic mail.

Layer 6: Presentation

Translates data from the Application layer into a common intermediary format. This layer also manages security issues by providing services such as data encryption, and compresses data so that fewer bits need to be transferred on the network.

Layer 5: Session

Allows applications on different computers to establish, use, and end a session. This layer establishes dialog control between the two computers in a session, regulating which side transmits, plus when and how long it transmits.

Layer 4: Transport

Handles error recognition and recovery. It also repackages long messages when necessary into small packets for transmission and, at the receiving end, rebuilds packets into the original message. The receiving Transport layer also sends receipt acknowledgements.

Layer 3: Network

Addresses messages and translates logical addresses and names into physical addresses. It also determines the route from the source to the destination computer and manages traffic problems, such as switching, routing, and controlling the congestion of data packets.

Layer 2: Data Link

Packages raw bits from the Physical layer into frames (logical, structured packets for data). This layer is responsible for transferring frames from one computer to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer.

Layer 1: Physical

Transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium. This layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable.

Each layer has the property that it only uses the functions of the layer below, and only exports functionality to the layer above. A system that implements protocol behaviour consisting of a series of these layers is known as a 'protocol stack' or 'stack'. Protocol stacks can be implemented either in hardware or software, or a mixture of both. Typically, only the lower layers are implemented in hardware, with the higher layers being implemented in software.

For more information see: http://en.wikipedia.org/wiki/OSI_seven-layer_model, http://www.lewistech.com/rlewis/Resources/james.aspx

Introduction to Routing

Briefly, **routing** is the process by which networks discover the paths along which information or data packets can be sent. Given the right information, networks can choose the best route to deliver data to a destination, based on goals such as finding the shortest distances and the fastest links available through a choice of network connections. This allows the network to route around network failures and blockages, and can make many aspects of the day to day running of such networks automatic, and free from the need for human intervention.

For more information see: http://en.wikipedia.org/wiki/Routing

A router is the physical device which sits at the connection point between different networks, enabling information to flow between them. Its size and sophistication depends on the amount of traffic it has to handle – from a simple device for a small office network to a massive stand-alone supercomputer that handles millions of data packets per second at major traffic points on the Internet. A router has two primary functions:

- Ensure that information reaches its correct destination.
- Ensure that information only goes to its correct destination and doesn't use network resources unnecessarily.

For more information see: http://computer.howstuffworks.com/router.htm.

More specifically, within a single logical network, the devices know how to resolve addresses using a Layer 2 (Data Link layer) protocol. For instance, most logical networks are built on top of Ethernet physical networks. Machines or routers are physically connected using switches or hubs ("repeaters") and each device on the network has a physical address – the MAC Address – associated with its layer 3 IP address. A protocol called ARP (Address Resolution Protocol) is used to resolve these IP addresses using physical addresses.

For more information see: http://en.wikipedia.org/wiki/Address_resolution_protocol, or http://www.faqs.org/docs/linux_network/x-087-2-issues.arp.html.

The boundaries of the logical network are defined by a network address and mask. The address is ANDed with the mask to identify the network and the mask determines the size of the network. First, last addresses usually have special meaning, with the last usually being the broadcast address used by link layer protocol.

If a device wants to communicate with an address falling outside its own logical network, it sends packets to its default gateway (router) which then (hopefully) forwards it on to another gateway until it reaches the logical network in which that address resides. The same logic applies to replies sent by this address. A route is the set of rules that determines where gateways should send packets. Each route is a tuplet consisting of a network (i.e. address/mask pair) and a gateway (IP address of router) to sent packets destined for the network to, but there are more routing metrics (rules) that can be used to determine the fate of a packet.

For more information see: http://www.faqs.org/docs/linux_network/x-087-2-issues.routing.html

Interior Routing Protocols

An interior routing protocol is a routing protocol that is used inside a network that is under a single administrative control (such as within a single ISP). In contrast, an exterior routing protocol is used between networks that are under different administrative control (such as between two different ISPs).

Static routes are the simplest interior routing protocol. They are convenient in a small network. As the network size and complexity grows, static routes become unmanageable. When there is a need for automatic failover to work around link failures or equipment failures, static routes do not work at all, and a dynamic routing protocol must be used.

There are several dynamic routing protocols available. OSPF and IS-IS are the two most recommended choices.

OSPF (Open Shortest Path First) is a very widely used dynamic routing protocol. The protocol is defined in open standards, and is implemented by almost all router vendors. We will use OSPF in this workshop.

IS-IS (Intermediate System-to-Intermediate System) is very similar to OSPF in the way that it works internally. It is not implemented by as many equipment vendors as OSPF. It is popular with some very large ISPs, and Cisco's IS-IS implementation has a very good reputation.

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol.

RIP (Routing Information Protocol) version 1 should never be seriously considered, because it is a classful routing protocol and cannot deal with the modern world of classless routing.

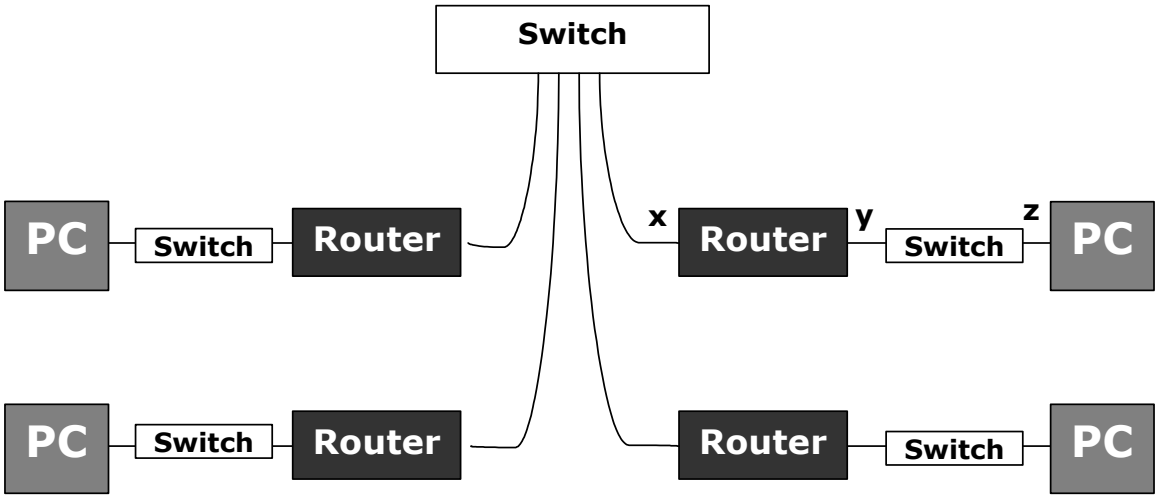
RIP version 2 is a classless version of RIP, but has serious performance problems.

Exercises

Exercise 1: Static routes

In this exercise, we will simulate a single ISP using static routes throughout its network.

Set up your equipment as follows:



a. The class is divided into teams. Each team has one router and one PC, plus cables, small switch, etc. All the teams are part of the same ISP, and will cooperate to make the entire network work correctly.

b. The instructor should assign a subnet to each team.

c. The instructor should assign a subnet to the backbone.

d. The instructor should assign individual IP addresses for connection from the router to the backbone (interface “x” in diagram).

e. Each team should assign individual IP addresses to other interfaces (“y” and “z”).

f. Configure each PC with its own IP address (“z”) and with a static default route (gateway = “y”)

g. Each router has a static route to each subnet associated with another team. If there are 6 teams, then each router will have 5 such static routes. In each case, the gateway is the other team's “x” IP address.

```
ip route <network> <netmask> <gateway>
! “network” and “netmask” refer to the other
! team's subnet. “gateway” refers to the
! other team's “x” IP address.
```

h. Once it works, use ping, traceroute, tcpdump, or other commands of your choice to verify.

Exercise 2: OSPF

In this exercise, we will convert the network from using static routes to using dynamic routes with the OSPF protocol.

Use the same network topology and addresses as for Exercise 1. Also retain all the static routes from Exercise 1.

a. Initiate a few long-running “ping”, “telnet”, “ssh” sessions (or any other protocol of your choice) to monitor stability of the network.

b. On each router, add OSPF commands to allow OSPF to start working in parallel with static routes.

```
router ospf 1
    passive-interface default
    no passive-interface ethernet 0/0        ! use the name of the backbone interface “x”
    network x.x.x.x  0.0.0.0                 ! use the IP address of interface “x”
    network y.y.y.y  0.0.0.0                 ! use the IP address of interface “y”
```

c. Verify with “show ip route” and “show ip ospf neighbor”.

d. Remove static routes one by one, verifying that OSPF routes take their place. Observe what happens to the long-running sessions as you do this (they should continue to work, although a few packets might be lost).