Technical Report IDE1042

Collaborating ISPs Supporting Various Real-Time Services

Master's Thesis in Computer Network Engineering

Ansar Zaman Cheema, Imran Ullah Saqib

School of Information Science, Computer and Electrical Engineering
Halmstad University

Preface

We are thankful to Halmstad University, they provided us required resources to accomplish our tasks in this project. We are also thankful to our supervisor Olga Torstensson for her teachings, encouragement and help in the project.

Ansar Zaman Cheema & Imran Ullah Saqib
Halmstad University, June 2010

Abstract

These days, internet service providers (ISPs) face the challenge about how to increase profitability while they must ensure a good quality service at the same time and scale up their network. The study involves previous research papers. On the bases of those papers, the comparison is made between different alternatives. The purpose on this study is to find a solution that combines different methods and configurations about how several ISPs could cooperate. Its implementation includes how different ISPs can configure their networks to cooperate on service provision supporting various real-time services.

Table of Contents

Chapter 1

1 Introduction

ISPs connect their networks to each other in order to exchange traffic between their customers and the customers of other ISPs. ISP Interconnection allows traffic originating at a source connected to one ISP's network to reach a destination connected to another ISP's network, around the block or around the world. End users see the seamless and global communication medium known as the Internet. Behind the scenes lay many individual networks, owned and operated by many different groups, institutional, and governmental entities, joined to each other by interconnection arrangements. Interconnection is the glue that holds the Internet together.

Interconnection enables the Internet as a whole to be fully connected. No single network operator could possibly provide Internet access in every part of the world. The model on which today's global interconnection arrangements are based has developed over the past three decades in parallel with the development of the Internet itself. Studies by a wide variety of public and private organizations have repeatedly concluded that it represents the most effective and efficient way to provide perfect public Internet connectivity.

Internet interconnection is fundamentally different from interconnection in the traditional circuit-switched telephony world. As a result, the nature of Internet interconnection agreements, the range of choices that are available for participants, the economics of interconnection and the variety of participants in the market are different from their counterparts in the telephony world.

1.1 Application Area and Motivation

The objective of this report is to describe how the Internet is made up of different entities of privately owned infrastructures, studies of Internet Service Provider (ISP) interconnection arrangements that have been performed from different perspectives, including the technical architecture, and the business and economic models that are the

result of peering and transit agreements. This report is intended to provide an historical context and concise summary of the evolution of ISP interconnection, how it was originated, developed, and practiced. The goal of this report is to describe the way in which the self-organized and self-regulating structures are designed that govern today's global Internet including the arrangements that enable ISPs to connect their networks to each other. These studies have been extensively reported and analyzed.

1.2 Approach Chosen to Solve the Problem

The methodology of this study involves both theoretical and practical implementation. The concept is taken from running ISP's infrastructure. To execute this idea, the material is obtained from previous research work. The analysis is made after extracting the information from research papers. This study provides the foundation for implementation, which is being carried out with available equipment. Configurations are presented in the appendix.

1.3 Thesis Goals and Expected Results

The goal is to describe the organized and well regulated structures that administrate today's Internet. It includes the arrangements that enable ISPs to connect their networks to each other. It has evolved naturally, over a long period, and according to principles that are deeply embedded in the Internet architecture. These structures are organized and well regulated because years of experience have shown that self-management is the most effective and efficient way to protect the valuable properties of the Internet. Our goals are:

1. To describe how different ISPs can configure their networks to cooperate with each other.
2. To describe the economic and management structures that describe the processes which govern today's Internet.
3. To find a solution that combines different methods and configurations to support real-time services when several ISPs cooperate.
4. The implementation and demonstration of the proposed solution.

1.4 Background

ISP collaboration is not a basic technical feature of the Internet. It is a management feature necessitated by the fact that the ownership and administration of the physical components of the Internet infrastructure are distributed among many different commercial, noncommercial, and governmental organizations. There is an important difference between internetworking and interconnection. Internetworking enables networks based on different telecommunication technologies and protocols to exchange data. Interconnection enables the owners and operators of different networks to collaborate as business entities in the provision of seamless, end-to-end Internet connectivity to all of their individual customers. Today, internetworking using the standard Internet Protocol is the common operating mode throughout the Internet. Interconnection takes place at public and private exchange points at which two or more ISPs make technical and administrative arrangements to exchange traffic.

Chapter 2

ISP Collaboration Overview

ISPs can be divided into three tiers of firms that target different customers, offer different services and have different structures of their networks. Tier 1, Tier 2 and Tier 3 ISPs.

Tier 1: These are large ISPs directly connected to the Internet backbone. They can be considered part of the backbone. They have very reliable networks and connections of the highest speed. Tiers 1's customers are lower tier ISPs like Tier 2 and Tier 3 ISPs. There can also be large companies that look for a reliable and fast internet access. The major advantage of purchasing service from this type of ISP is that solutions of the problems are much easier because only a single company is involved.

Tier 2: These ISPs purchase Internet service from a tier 1 ISP. The goal of Tier 2 ISPs is to cover a specific region. Mostly, they have business customers. They provide slower connection and lower quality than Tier 1 ISPs.

Tier 3: These ISPs can purchase Internet service either from Tier 1 or Tier 2 ISP. Tier 3 ISPs focus on the retail market and they do cover a specific region. Network quality and speed is comparatively lower. Prices are also lower than higher tier ISPs [1].

A transit ISP can only be the higher tier ISP but peering is made between same tier ISPs. Our study focuses on tier-1 and tier-2. Where tier-1 is a provider and transit for both tier-2 ISPs. Both tier-2 ISPs are customers of tier-1 and having peering relationship between them. Figure 1 and 2 shows the hierarchy of ISPs and relationship between them:

Figure 1: ISPs classification according to their strength on the globe

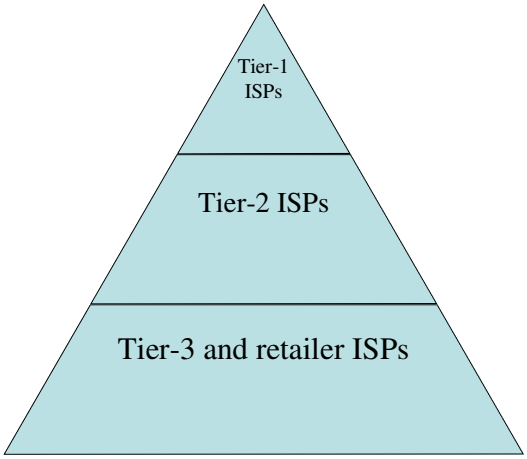
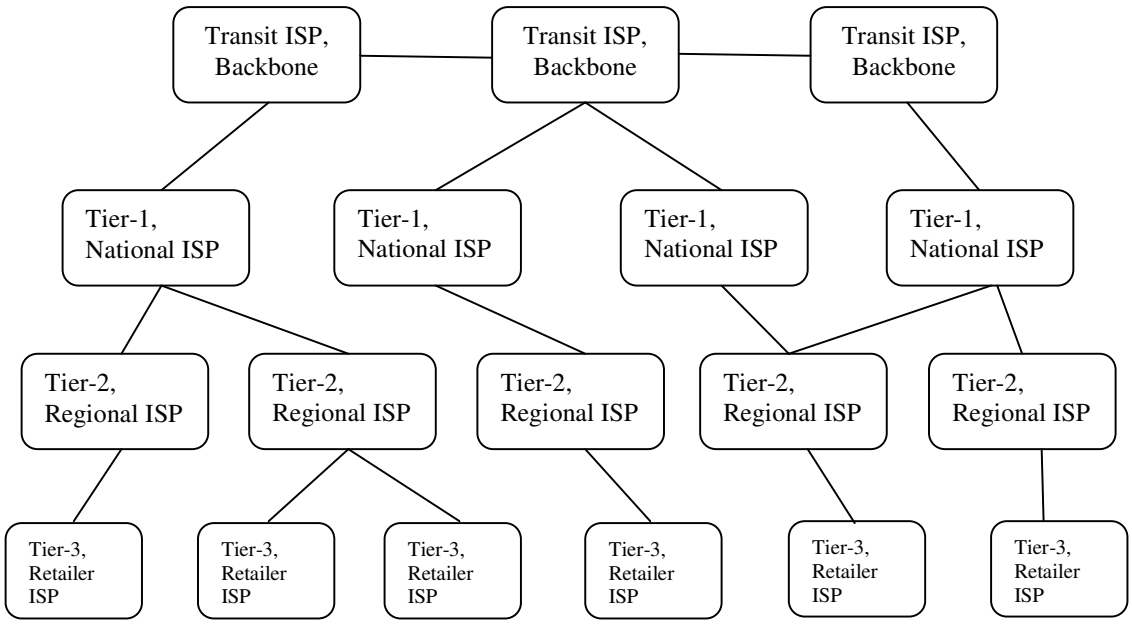


Figure 2: Provider to client hierarchy between ISPs



2.1 Peering and Routing between ISPs

The connectivity of nodes on the Internet is provided by the interconnection of many ISPs. This peering of ISPs with each other defines a set of transit relationships. These transit relationships are BGP-based inter-domain routing. This can be considered economically efficient. Here, we study models to represent P2P traffic demands, peering and routing in a market place of two competing ISPs.

The Internet is operated by ISPs who decide to interconnect their networks. There is a set of transit service agreements between ISPs. These transit agreements determine that how traffic flows between ISPs' networks in the Internet. There are two kinds of peering relationships between Internet ISPs. The first is the provider to customer relationship and the second is the peer to peer relationship, also called "free peering".

In a provider to customer relationship, the customer ISP pays the provider ISP for connectivity to the Internet. So the provider ISP provides free transit service to the customer ISP. The customer ISP also needs to provide some transit service to the provider ISP to reach the customer ISP or its customers but not to any other destinations. So the customer ISP provides a selective transit service [2].

In a free peering relationship, the traffic exchange on the peering link is almost free of charge. Only the traffic between the two peering ISPs and their customer ISPs can be exchanged on the free peering link. Such exchange of traffic helps both peering ISPs to reduce the dependence on their providers ISPs for transit service and it is economical.

Peering ISPs provide selective transit services so they rely on BGP that is a policy-based routing protocol that enforces selective transit agreements. An ISP's routing policy includes import routing policy and export routing policy. Import policy is applied to a neighbor that determines what transit service the local ISP is to accept from the neighbor. Export policy is applied as a filter to routes sent to a neighbor that declares what transit service the local ISP is offering to that neighbor [3].

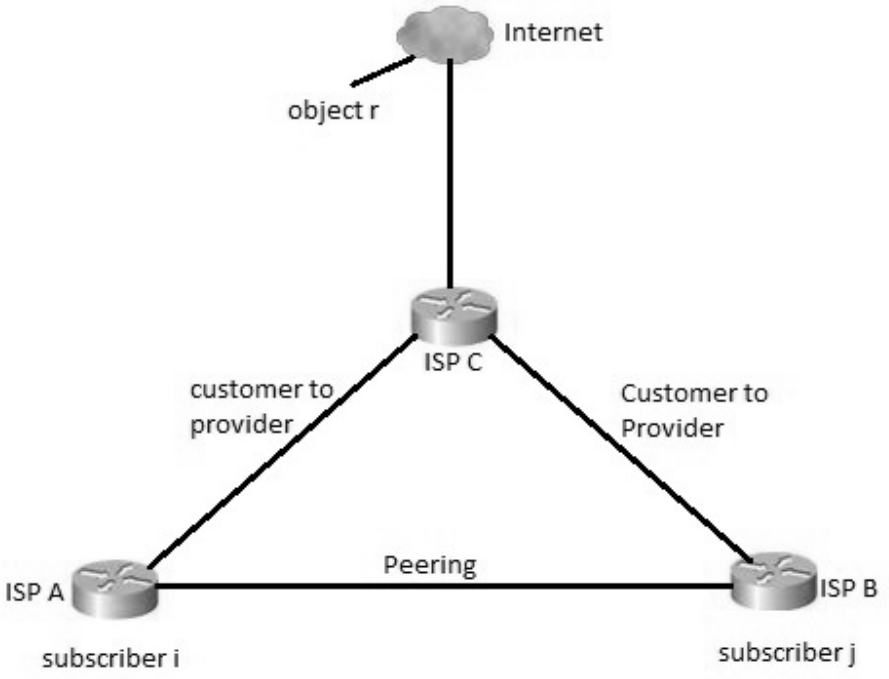
2.2 Real Time Example

There are three Internet service providers ISP A, ISP B and ISP C. ISP C is provider ISP and ISP A and ISP B are customer ISPs. Customer ISPs set up a free peering link to reduce the transmission cost on their network that they pay to ISP C beforehand. So there is a triangle of connections. In this network, if a subscriber A of ISP A needs an object R from Internet, the information flow is transited through ISP C and arrives at ISP A for subscriber A. Due to policy-based routing, the object cannot have the path (Internet > ISPC > ISPB > ISPA) since ISP A does not receive the route to object R from ISP B under the free peering agreement.

We can assume that routing of such peering agreements is economically efficient. Such an economically efficient scenario, however, is not the best possible service for individual subscribers and the applications they are running for a lot of reasons. One reason is that it would be too complicated for the network layer to learn about the application requirements and its routing [4] [5].

Peer-to-peer (P2P) applications can conflict with ISP controlled routing. To provide efficient distribution of data to many receivers, peers play the role of information receiver as well as server. As an example, the object R is a P2P object in the Internet and it is needed by both subscriber A and subscriber B. To improve performance, a P2P application makes both subscribers A and B provide service to each other. So, subscriber A may receive some pieces of object R from subscriber B. If we look at the routing of the pieces from subscriber B to subscriber A at the application layer, they traverse along the path (Internet > ISPC > ISPB > ISPA). The traffic on the peering link is beneficial only for ISPA. ISPB is providing transit service for ISPA without being paid by ISPA, which is not according to the peering agreement between ISPs. This example describes the routing tussle between ISPs and P2P applications. So the question is, which ISP gets more benefit from this free peering? Our main contribution is to focus on this problem using relatively simple models. We also find alternative peering and their effectiveness [6].

Figure 3: Peering between ISPs



2.3 Networking

Neither internetworking nor interconnection were features of the Internet in its formative stage of development. Before LANs and PCs, computer communication meant connecting I/O and storage peripherals, such as card readers, terminals, and printers, to definitely self-contained mainframe computers. Early ways to connect computers to each other led to networks based on a variety of different proprietary communication technologies and protocols. They designed a "distributed communications network". When there were just a few of these homogeneous networks, it was possible to exchange information between them by building a translator. However, as the number of networks grew, the n-squared scaling inefficiency of pair-wise translation led to the idea of internetworking that creates a network of networks.

2.4 Internetworking

It is remarkable to realize that the very earliest thinking about what a "network of networks" an "internet" should be embraced the three key concepts that underlie the architecture of today's global Internet:

1) The concept of packet switching originated in at least three distinct places during 1961-1965. They concluded that the strongest communication system would be a distributed network of computers with (a) redundant links; (b) no central control; (c) messages broken into equal-size packets; (d) variable routing of packets depending on the availability of links and nodes; and (e) automatic reconfiguration of routing tables after the loss of a link or node.

2) The concept of best-effort service, which originated in the multi-access channels.

3) The concept of application independence, that the network should be adaptable to any purpose, whether foreseen or unforeseen, rather than tailored specifically for a single

application (as the public switched telephone network had been purpose-built for the single application of analog voice communication) [7].

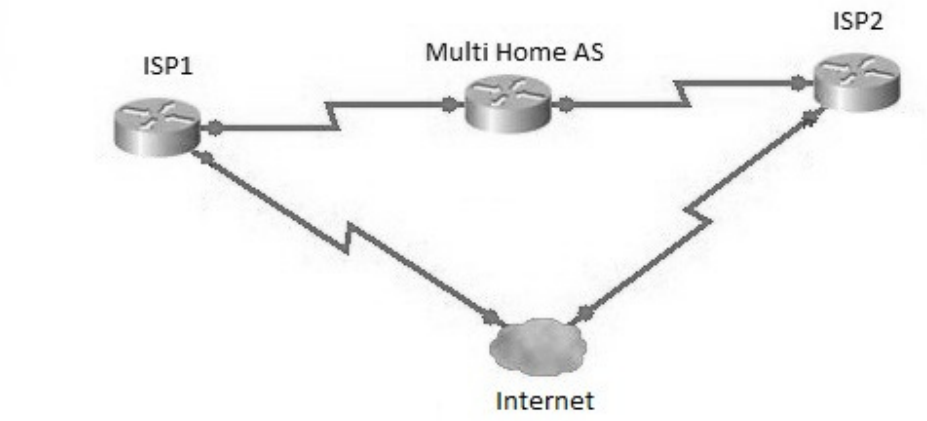
2.5 Autonomous Systems

An autonomous system is a group of routers under common administration that share the same routing policy is known as “autonomous system” (AS). Each AS has 16 bit number assigned by internet routing registries [13]. An AS’s numbers are divided into two categories with respect to ranges: Public (1-64511) and Private (64512-65535). Autonomous systems can be single-home AS or multi-home AS.

Single-home reaches networks outside its domain through a single exit point. In multi-home AS, transit and non-transit relationships can be established with another AS or another ISP. In transit relationships, AS is allowed to pass traffic from another AS. In non-transit relationship ASs do not act as a transit between ASs. They blocks all traffic.

Figure 4: Shows connection between single home AS and ISP.

Figure 5: Shows the connection of Multi-home AS to different ISPs.



Chapter 3

BGP (Border Gateway Protocol)

3.1 Introduction of BGP

BGP is an inter-domain routing protocol that is based on the path-vector routing method. The path is a list of ASs that a packet should follow to reach the destination network. BGP creates its routing table for each route object. The BGP table carries information about address prefixes and associated path lists. The purpose of BGP is to exchange network reach-ability information and information about the list of AS paths with other BGP peers. BGP is a highly scalable protocol that is used to manage large Internet networks with big routing tables. BGP uses TCP at the transport layer to provide a reliable communication. BGP is commonly used between ISPs. The primary function of a BGP speaking system is to exchange the network information with other BGP systems regarding reachability. Some policy decisions at the AS level might be enforced. BGP plays a key role on the Internet. It interconnects ASs, each with a unique number (ASN), and facilitates the construction of routing tables. Each AS has one or more BGP speakers that exchange reach-ability information with other speakers located in neighboring or peer ASs. For example, a speaker may receive the following reach-ability information from peer AS-1384: [130.130.0.0/16 → {1384 38 383 211 666}], which indicates that AS-1384 has a route to the network 130.130.0.0/16, via the ASs: {1384, 38, 383, 211, 666}. Hence, by exchanging reach-ability information, each speaker is able to construct a routing table containing paths to various destinations on the Internet [8].

There are two types of implementation of BGP.

Internal Border Gateway Protocol (IBGP): BGP that runs inside same AS is known as "interior border gateway routing protocol".

External Border Gateway Protocol (EBGP): BGP that runs between different ASs is known as "exterior border gateway routing protocol".

3.2 BGP Path Attributes

Path attributes are a set of parameters that BGP uses to create routing policy and filtering. BGP path attributes are divided into four categories:
Well-known mandatory
Well-known discretionary
Optional transitive
Optional non transitive

All BGP routers recognize well-known attributes. Well-known mandatory attributes must include in each BGP update message and a well-known discretionary attribute may or may not be added into a BGP update message. It is not necessary that all BGP routers do recognize optional attributes. Optional attributes may or may not be included in every message update. BGP routers may allow optional transitive attributes to pass through, but a BGP router does not allow optional, non transitive attributes to pass other BGP routers.
AS-path: AS path attribute is well-known mandatory. The AS-Path is a list of ASs that a route passes through to reach the destination. A list of ASs is displayed in the AS path attribute. The route that has fewest AS numbers in its path list is selected as the best route. AS-path also provides loop prevention. For example, if an AS number received its own AS number in the AS-path list, that route will be dropped.
Origin: Origin is also a well-known mandatory attribute. It defines the origin of route information.
Next-hop: This is a well-known attribute that gets the IP address of the next border router. The next-hop IP address changes as the route passes through different ASs because each AS has a different next hop. The operations of the next-hop attribute are different in the case of IBGP and EBGP.
Multi-Exit-Discriminator (MED): MED is an optional non-transitive attribute. The MED attribute is a value that is given to the routes when more than one entry point exists into AS. This attribute is used to select the best path for inbound traffic coming to AS. The path that has the lowest value of MED is preferred and the default value is 0.
Local-Preference: Local Preference is a well known discretionary attribute. It

describes the IBGP peers' preference for an advertised route. The distribution of this attribute is local to AS.

Atomic-aggregate: Atomic-aggregate is a well-known discretionary attribute. The atomic-aggregate attribute is used to notify neighbors about routes that become invalid or are dropped due to aggregation.

Community: Community is optional transitive attribute. The community attribute has a 32 bit integer value used to group the number of destinations. Each destination can be in more than one community. Tags are used to carry information about the routes within the AS or between ASs. This attribute is very handy for applying the routing policy, as communities are grouped into various kinds according to their description of path attributes. There are some well-known communities, like no-export, no-advertise and no-export Sub conferred.

Aggregator: Aggregator is an optional transitive attribute. It contains information about last AS and IP addresses of BGP peers that advertise the aggregate route [9].

3.3 BGP Messages

There are 4 types of messages that are exchanged between BGP to establish relationships and relaying of routing information. As BGP does use TCP for transportation at port 179, common header of BGP messages consist of 16 bytes marker, 2 bytes length and 1 byte type that limits the message size to 19 bytes. The type field defines the message type. At the time of initialization, the whole routing table is loaded and only incremental updates are exchanged. There are no periodical updates for the BGP states.

The BGP messages are as follows:

Open Message

Update Messages

Notification Message

Keep Alive Message

The open message is sent to start a BGP session among BGP peers. This message is used to identify BGP peers by verifying local AS's number, the local version and other

optional attributes. The BGP exchanges routing information with neighbors via an update messages. The update message contains information about the update prefixes and withdrawn prefixes. An established BGP session remains open for the limited time span to exchange routing information; if an error occurs during the usual communication of peers, the session is terminated. Some errors which are critical result in the termination of the BGP session immediately. The error warning is sent through the notification messages. A hold timer starts an update message that is received to ensure that some activity is in progress. If the hold timer expires, the BGP session will be non operational. To keep the BGP session operational, a keep-alive message is sent after every 60 seconds. If a BGP peer does not receive any keep-alive message, it closes the session.

3.4 Characteristics of BGP

The most important characteristics of BGP is flexibility. The protocol can connect any internetwork of any autonomous systems by using an arbitrary topology. The only requirement is that each AS must has at least one router that is BGP compatible and the router is connected to at least one other BGP router of its AS. BGP is able to handle a set of ASs connected in a full mesh, partial mesh topology and a chain of linked ASs. It can also handle changes to the topology that may occur over time. The further characteristics can be divided into short points. These points are described below.

The other main characteristics of BGP are its routing updates. In BGP updates, you can see BGP is excellent for communicating between autonomous systems. BGP works as an exterior routing protocol because the routing updates are extremely concise. The BGP routing update takes summarization to the extreme by communicating only a list of autonomous systems [10].

BGP is a path vector routing protocol and it uses hierarchical addressing that has the ability to manipulate traffic flow that results to growth of the network design.
As it mention above that it has its own routing table, although it is capable of both sharing and inquiring about the interior IP routing table. It maintains a table of IP

networks and makes it possible for the ISPs to get connected with each other and be able to connect to more than one ISP for the end-users.

3.5 BGP Operations

BGP's operation can be described in the form of messaging. This allows the knowledge about how to reach networks to spread in the internetwork. BGP is connection-oriented; a TCP peering session is established and maintained when a neighbor of router is seen. Before the messaging begins, BGP speakers must be designated and linked. BGP standards do not specify how the speakers are determined in neighbor. This is done outside the protocol. The routers then send incremental updates only when changes occur. The update refers to a single path and the networks that can be reached via that path.

BGP operation begins with BGP peering that forms a transport protocol connection. The operation of a BGP is very simple. Indeed, all the complexity of the protocol is delivered in only a few different message types in which each BGP speaker sends a BGP open message. There are different message types that are used in BGP:

The open message is used to establish connection between peers. It tells its peer what parameters it would like to use for the link. This includes an authentication parameter's exchange. Assuming that each device does find the contents of its peer's open message acceptable and acknowledges it with a keep alive message and the BGP session begins.

3.6 BGP Routing Policies in ISP Network

BGP was born out of the need for ISPs to control route selection to forward packets and propagation who to export routes to. However, ISPs found it useful and started to modify routing configurations [9]. BGP was a simple path vector protocol. It was modified incrementally over time with a number of mechanisms to support policies. To address the BGP's complexity is difficult when there is certain aspect of BGP. For example, changing the contents of update messages or the way they are propagated must be

coordinated and separately implemented in other ISPs to support the new design. In order to understand BGP, it is necessary to understand the process of decision making and the policies of ISPs that enabled its design to grow. Understanding policies is also key to solving BGP's problems, understanding measurement data from BGP, and determining what features to support when developing a new version of BGP.

BGP is the routing protocol used to exchange reachability information across ASs. So each ISP operates one AS, though some ISPs may operate multiple ASs for business reasons to provide more autonomy to administrators of an ISP's backbone. The Internet consists of thousands of AS networks that are each owned and operated by a single institution. Non-ISP business enterprises may also operate their own ASs so as to gain the additional routing flexibility that arises from participating in the BGP protocol[11].

Chapter 4

IP Multicasting

Real-time services in which ISPs may cooperate can be multimedia applications that integrate sound, graphics, animation, text, and video. These types of applications have become an effective means of group communication. Sending combined media over a site data network requires a lot of bandwidth. IP Multicast is a resourceful way of delivering media to many hosts over a single IP flow. IP multicast includes an addressing set, methodologies for the users of multicast to become members of groups, source and shared trees, and multicast routing protocols.

Multicast routers have to know the origin of the packet rather than its destination. In multicast initiation, the group of receivers is denoted by destination IP address. The decision of forwarding the multicast packet depends upon the source of the packet. Multicast routing uses a mechanism that is called “reverse path forwarding”, also known as “RPF”, to prevent forwarding loops. RPF finds the shortest path to receiver from source [12].

4.1 Multicast Groups

Multicast is used to send the same data packets to multiple receivers. A multimedia server sends one copy of each packet to a single end IP address that can be received by many end stations if they choose to listen to that address. The video server transmits a stream of video signals to a set of host devices listening to a specific multicast address. Server-to-network bandwidth utilization is only 1.5 Mbps, not considering the number of receiving hosts. By sending the data packets to multiple receivers, for every receiver the packets are not duplicated, but are sent in a single stream. When necessary, downstream routers perform packet multiplication over receiving links.

Routers process fewer packets because they receive only a single copy of the packet. Downstream routers perform packet multiplication and delivery to receivers, the sender, or the source of multicast traffic, so they do not have to know the unicast addresses of the receiver. In Simulcast, simultaneous delivery for a group of receivers may be used for numerous purposes, including audio or video streaming, news and similar data delivery, and software upgrades. To send data to multiple destinations using unicast, the sender has to send the same data flow to each receiver separately. The sender has to make copies of the same packet and send them once for each receiver.

Web technologies like webcasting use a “push” method to deliver the same data to multiple users. Instead of users clicking a link to get the data, the data is delivered repeatedly. Users have to subscribe to a channel to receive the data. After that the data is periodically pushed to the user. The problem with the webcast is that the transport is done by using unicast.

4.2 Difference between Unicast and Multicast

In unicast transmission, multiple copies of data are sent, one copy for each receiver, for example, there will be a host transmitting three copies of data and a network forwarding each packet to three different receivers. The host may send to only one receiver at once, because it has to deal with a different packet destination address for each receiver.

In multicast transmission, it sends a single copy of the data to the multiple receivers. The data is sent to the multicast receivers because they have already subscribed to receive it. For example, a host transmits one copy of the data and a network replicates the packet at the last possible hop for each receiver. Only a single copy of packet exists on any given network. The host sends to multiple receivers simultaneously because it is sending only one packet. Downstream multicast routers replicate and forward the data packet to all the places where there may be receivers.

4.3 Multicast Transmission Advantages

Multicast provides many advantages over unicast in a one-to-many or many-to-many environment.

It enhances efficiency. Network bandwidth is utilized efficiently because multiple streams of data are replaced with a single transmission.

It optimizes performance. Fewer copies of the data require forwarding and processing.

It distributes applications. Multipoint applications will not be possible with unicast as required and usage grows, because unicast transmission does not scale traffic level and clients increase at a 1:1 rate with unicast transmission.

For the equal amount of multicast traffic, the sender uses less processing power and bandwidth.

Multicast packets do not require as high a rate of bandwidth utilization as unicast packets. There is a greater possibility that they will arrive at their destinations almost simultaneously.

Multicast enables a whole range of applications that were not possible on unicast like video on demand.

4.4 Multicast Applications

There are many types of multicast applications. Here, three of the most common models are described.

One-to-many is where a sender sends data to many receivers. This type of application is used for audio or video distribution, push media, announcements, monitoring etc. If a one-to-many application needs responses from receivers, it becomes a many-to-many application.

Many-to-many is where a host acts as a sender and a receiver at the same time or where more than one receivers acts as a sender. Receiving data from several sources adds more complexity in applications and creates different management problems. Using a many-to-many multicast concept as a base, a whole new range of applications is built, for example, collaboration, concurrent processing, and distributed interactive simulations.

Many-to-one is where many receivers send data back to one sender. It is most commonly used by financial applications and networks. Other uses are resource discovery, data collection, auctions, and polling.

Many new multicast applications are emerging as demand grows. Real-time applications can be live broadcasts, financial data delivery, whiteboard collaboration, and videoconferencing. Non real-time applications are file transfer, data and file replication, and video on demand. Ghosting multiple PC images at the same time is a common file transfer application.

4.5 IP Multicast Addresses

Routers differentiate multicast traffic from unicast or broadcast traffic by using the reserved Class D IP address space. Network devices can pick out Class D multicast IP addresses by looking at the four, most significant, high-order bits, that are always 1110. The following 28 bits are referred as the group address.
Range of IP multicast addresses is from 224.0.0.0 - 239.255.255.255.
Multicast IP address space is divided into the following address groups.

Locally scoped addresses
It is reserved by the Internet Assigned Numbers Authority (IANA) for network protocol use. The address range is from 224.0.0.0 - 224.0.0.255. Multicasts in this range are never forwarded off the local network, apart from time to live (TTL). TTL is set to 1.
Globally scoped addresses
These are allocated dynamically throughout Internet. The address range is from 224.0.1.0 - 238.255.255.255. The 224.2.X.X range is used in multicast backbone applications also known Mbone. Developed by the Internet Engineering Task Force (IETF), to multicast audio and video meetings. Mbone is a collection of Internet routers that support IP multicasting. On bases of these, various public and private audio and video programs are sent.

Limited scoped addresses

These are reserved for use of inside private domains. The same as private IP address space that is used within the boundaries of a single organization. These administratively reserved addresses are constrained to a local group or organization. The address range is from 239.0.0.0 - 239.255.255.255. Organizations use limited effective addresses to have local multicast applications that are not forwarded over the Internet.

Within an autonomous system, the address range that has limited scope can be subdivided. Local multicast boundaries can be defined this way. This subdivision is called “address scoping” and allows the re-using of addresses between smaller domains. The administratively scoped multicast address space is further divided into the following scopes:

Organization Local Scope (239.192.0.0 to 239.251.255.255)
Site Local Scope (239.255.0.0/16, with 239.252.0.0/16, 239.253.0.0/16, and 239.254.0.0/16 also reserved)

4.6 IP Multicast Sessions

When a multicast application is started on a receiver, the application must know which multicast group to join. The application must learn about the available sessions or streams, which map to one or more IP multicast groups. There are different ways that applications can learn about multicast sessions:

The application joins a known predefined group to which announcements about available sessions are made. The application contacts with a proper directory server.
The application is launched from a web page where the sessions are listed as URLs. Even email may be used.
The user configures the application to listen to a multicast session by manually entering the IP multicast address within the application.

The session directory (sd) application works as a guide and displays multicast content. The client application runs on a PC and lets the user know what content is available. This directory application uses either session description protocol (SDP) or session announcement protocol (SAP) to learn about the contents.

4.7 Protocols Used in Multicast

Multicast distribution trees define the path from the source to the destination over which the multicast traffic flows. There are two types of trees of multicast distribution.

Source tree is a separate tree that is built for each source to all of the other members of its group. A source tree takes the shortest path from the source to its receivers; it is called a "shortest path tree", also known as SPT. Each source pair requires its own state information. The groups that are having very large number of sources or nodes that are having large number of groups with a large number of sources in each group. Source trees may cause the requirement for more storage capacity of routers.

Shared tree protocols create multicast forwarding paths relying on central a core router. That is actually a rendezvous point (RP) between multicast destinations and source. Initially, the source sends the multicast packets to the RP. It forwards data through a shared tree to other group members. Paths between the source and receivers may not be the shortest. However, it is less demanding for memory and the CPU on routers. There are basically two types of modes of multicast routing protocol: Dense Mode (DM) and Sparse Mode (SM).

Protocols in Dense mode do flood the multicast traffic throughout the network and reduce the flows where there are no receivers, using a periodic flood and prune mechanism.
Sparse mode protocols use an open join mechanism where distribution trees are built on demand by explicit tree join messages sent by routers that have directly connected the receivers.

4.8 PIM Dense Mode (PIM-DM)

PIM-DM initially floods traffic out of all non RPF interfaces where there is another PIM-DM neighbor or a directly connected member of the group. Multicast traffic is sent by the source that floods to the entire network. Routers receive the multicast traffic via the RPF interface. This interface lies in the direction of the source. It forwards the multicast traffic to all of its neighbors using PIM-DM. Traffic that arrives via non-RPF interface is discarded. These flows are normal for the initial flooding of data and corrected by the PIM-DM pruning mechanism. Pruned messages are sent on non-RPF interfaces to cut off the flow of multicast traffic, because it is arriving via an interface that is not the shortest path to the source. Pruned messages are sent on an RPF interface when the router does not have any downstream receivers for multicast traffic.

Although the flow of multicast traffic does not reach most of the routers in the network anymore, this state remains for all of them and will remain until the source stops sending. All pruned messages expire in 3 minutes. After that, the multicast traffic is flooded again to all the routers. This periodic flood and prune behavior is normal and has to be taken into account when the network is designed to use PIM-DM [13].

Chapter 5

The Service Level Agreement

The SLA defines the limitations of the autonomous nature of ISPs. There are different methods of extending the SLA that are offering across ISP boundaries: Least Effort, Most Effort and Equal Distribution Policy. These were introduced to coordinate end to end performance guarantee in multiple ISP networks. Different manners are associated with these policies in which service level constraints are distributed in all transit networks. When SLA is required, we study how much these policies affect the entire ISP community. The effectiveness of these policies in terms of network performance and ISPs' monetary profit will be evaluated. Policy choice depends on network load and ISP cost structure.

An ISP makes contracts with its customers' SLA. SLAs serve to ensure that the service providers maintain a specific level of service. The service providers benefit from SLAs because SLAs permit differential treatment of the customer traffic. Differential treatment of customer traffic can yield economic benefits to the service providers like, for example, not having backup for all connections. This method allows for the service providers to get maximum benefit from their available resources, and the customer opts for SLA guarantees because they can ensure the rigid level of performance they pay for, and be compensated for the lack thereof. Also, SLAs also provide a financial attraction for the customer since he need not subscribe to, and hence not pay for, unwanted services.

5.1 SLA guarantee across multiple ISPs

Currently, no SLAs are offered beyond network boundaries by any of the ISPs. Some of the reasons for this are discussed below:

5.2 Undisclosed network information

Provisioning schemes rely on network-wide topology and resource information. Such

information has been considered by the ISP as confidential and never disclosed. This is cleared from the exterior gateway protocols for routing across ISP networks. The exterior gateway protocol, such as BGP, covers the internal topology details and advertises reach ability of network addresses and dynamic behavior of such address to neighboring networks. It is difficult to achieve end-to-end computation without the global link state information.

5.3 No SLA interconnection policy

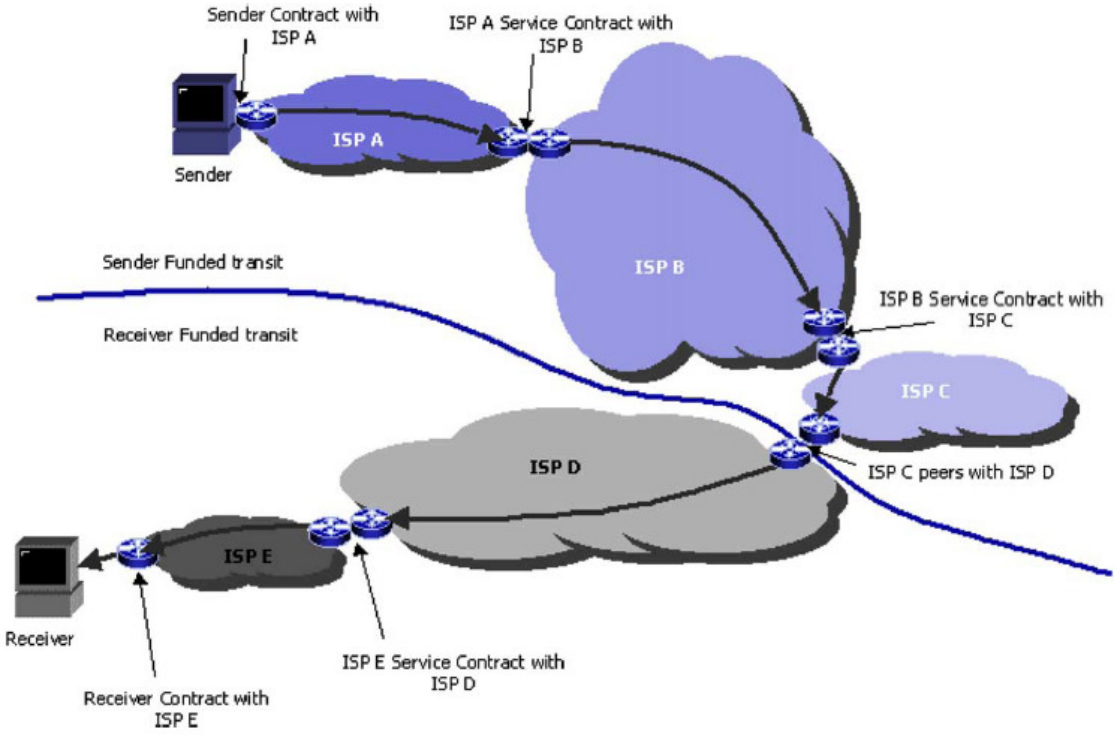
In order to provide for a connection across multiple ISP networks, each ISP network must provide a path for the connection locally. This task can be achieved by the algorithms. The challenge is to provide an interconnection mechanism. This can be explained with an example. Suppose two ISPs having relative classes of service, such as gold, silver, and bronze. The service-level parameters of the gold class in one ISP may not necessarily be the same for the gold class in another ISP and, if the service-level parameters in each traffic class are not disclosed, there is no way to provide guarantees for adjacent ISPs. Even if the constraints were disclosed by ISPs, maintaining requested parameters from end to end is a daunting task and coordination among all transiting ISPs. The design of the interconnection policy should allow it to calculate how to apportion the SLA constraints to each local provisioning. For constraints like maximum bandwidth, this is not a problem as the threshold will remain the same for all transit networks but may be a problem for additive constraints, such as maximum delay and jitter, or for multiplicative constraints such as reliability and availability; the manner in which these thresholds are distributed could greatly affect the feasibility of the end-to-end performance offering.

5.4 Lack of supporting ISP business model

The lack of financial incentive is another difficulty faced by the service providers. At present there exists no end-to-end pricing scheme that is able to support guaranteed services. Commonly financial settlement between two ISPs may be categorized as peer, wholesale service, and retail service. Peer ISPs do not charge each other for traffic

exchange. Wholesale ISPs charge each other on the basis of traffic volume and not quality. As no financial incentive is offered for increased performance, wholesale ISPs will not offer any guarantees. Retail ISPs charge fees according to the levels of quality they offer however still they cannot guarantee the same level of performance outside their own boundaries. Figure 3 explains how different ISPs interact with each other to provide an end to end connection. [14]

Figure 6: ISPs' interconnections from sender to receiver



Chapter 6

Pricing

These days, Internet service providers (ISPs) have to face the challenge of how to increase profitability while they ensure a good quality service at the same time while they scale up the network. The Internet is made up of different entities of privately owned infrastructures. Generally, there are two types of network service providers: 1) local ISPs, which are geographically close meshed networks and provide Internet access and connectivity services within their local area of operation, and 2) large-scale ISPs, which have a large geographical separation in their end-to-end users.

Usually the local ISPs gain the Internet access by purchasing this service from higher level ISPs (or transit ISPs). The transit ISPs charge a service provisioning charge which depends upon the amount of bandwidth allocated and the amount of traffic transferred. A challenge these days is to come up with a pricing model that ensures the judicious distribution of earnings according to the services rendered. A flat rate system is adopted by most ISPs these days, which means that there is a fixed charge for Internet services for a definite amount of time. Common examples of the flat rate system include most broadband and ADSL services. The other approach is to charge users by the time they are connected to the internet following the model based on the telephony industry. There are also some ISPs who charge users based on the actual amount of traffic volume transmitted. There is already some work available that discusses various pricing strategies for ISPs.

Local ISPs can bypass transit ISPs for Internet access and interconnect their networks by signing up private peering agreements. Geographically close local ISPs can exchange information between themselves. One possible way to accomplish this is to establish a private peering link between two parties. The formation of private peering agreements is quite difficult and requires quite a few business considerations; however, in its most basic form the private peering is designed for the transfer of traffic between two ISPs without

paying them the cost of transfer. It should be noted that free peering is just one form of the peering arrangement and a charge may be implemented in some arrangements. This method usually leads to lower costs and higher performance for both ISPs.

Here, efforts have been made to find out how to set Internet prices to ensure the fair distribution of profits and allow the Internet to grow at the same time. In these works, however, the impact of local peering relationships on traffic has been underestimated, as having local peering will consequently lead to the proper pricing strategy and in turn, to maximizing profits. The challenge is to aim at bridging this gap by exploring how the peering relationship can affect the service purchasing strategies and pricing strategies played by ISPs.

Two options are available to a peer in order to communicate with another local ISP: to use of a connection provided by transit ISPs or to use the peering link connecting the two peers. Even if given a constant transmission demand, deciding upon an appropriate proportion of traffic delivered via these two connections is not an easy matter. So one peer's optimal strategy may be regulated by the strategies taken by other peers and the pricing policy employed by the ISP. This makes it an impossibly difficult task to come up with an efficient resource allocation plan.

Internet access and connectivity between peers is provided by the ISP. Revenue maximization by providing connectivity service is the goal of the ISP. A good pricing strategy is essential in order to maximize the total profit and attract more potential peers. Generally, the following issues need to be addressed by a transit ISP:

6.1 Resource distribution

The ISP should come up with a method to allocate and sell its capacity to competing users and avoid monopolization of bandwidth by a small number of peers.

6.2 Maximization of revenue

Find out an optimal price which reaps maximum revenue for the ISP and provides a unique and homogeneous pricing strategy. If it exists, how can one find this optimal price.

6.3 Upgrade of capacity

Increasing demand for Internet access will lead to more peers entering the market. There is enough incentive for the ISP to upgrade the network infrastructures (increase the backbone capacity) to accommodate more peers.

6.4 Impact of peering relationship

The ISP does not want monopolization of its bandwidth by a small number of peers since it prefers to diversify its peers. Attracting or retaining a peer for a connectivity service requires the ISP to perform a "fair" resource distribution, which avoids resource monopolization. The ISP achieves this goal by exchanging traffic information with its peers. Due to business confidentiality and the necessity to perform resource allocation in a distributed manner, minimal information exchange takes place. On the other hand, profit maximization is also another ISP objective. Since the price influences how much traffic a peer decides to transmit via a transit ISP, the aggregate traffic thus determines the total demand on the ISP link. Even though setting a low price may attract more peers, it may also lead to congestion. Moreover, a low price does not guarantee the maximization of the ISP's revenue. On the other hand, setting too high a price may discourage peers from purchasing the ISP service and, therefore, decrease traffic demand, which fails to ensure the achievement of maximum profits for the ISP as well. Therefore, finding an optimal unit price is an important issue. [15]

Chapter 7

7.1 Detailed Description of the Investigated Solution

The study proposes the routing policy of BGP configured network between ISPs and protection from malicious traffic. The configuration of BGP in peering and transit networks is a complex procedure. This routing policy provides the security features of BGP and provides a solution to configure BGP in a secure way. Cisco routers and switches are used in implementation of practical environment. Most of the ISPs use Cisco devices at the core, and distribution and access layers in their domains. Implementation design has two routers in each ISP domain connected to the Internet. These routers are responsible for the filtration of traffic from neighbors. It will result in an effective configuration of real time scenarios for complex transit and peering networks providing real time services.

We have used protocol independent multicast (PIM), that is family of multicast routing protocols but we implement dense mode. PIM is protocol independent, it does not have its own discovery mechanism. It uses routing information provided by other routing protocols, as BGP has been used in this scenario. PIM dense mode uses dense multicast routing that builds the shortest path tree by sending the multicast traffic domain wide.

Multicast routing protocol enables routers to deliver copies of multicast packets efficiently to the receivers. In this process, the multicast routing protocol provides a mechanism for discovering the neighbors and to track neighbors' routers that are also using the multicast routing protocol.

The computers which are interested in receiving a multicast packet stream do use Internet group management protocol (IGMP). It is used to notify adjacent routers. The purpose in using this protocol is to arrange a copy of the multicast packet stream to be sent to them so that they can forward it. At the source end of the packet stream there is no protocol to

communicate, register or notify to the routers. Once the source starts sending the packets to the neighbors, it is up to the neighbors' routers to do rest of the job.

In contrast with PIM Sparse Mode (PIM-SM) that has not been used, it assumes there are relatively fewer receivers. An example can be the initial orientation video for new employs or Video on Demand (VoD).

As we use BGP as extension for IP Multicast. It adds the capabilities to BGP to enable multicast routing policy throughout the entire Internet. BGP connects multicast topologies within the AS and between BGP ASs. This combination make it enhanced BGP that carries IP multicast routes. BGP deals in two sets of routes, unicast routing and multicast routing.

This solution combines some features of the network like filtration of routes, managing neighbors and management of single home or multi home customers. For single home customers BGP is not configured for routing. As they have single exit point, they need default routes to communicate with their ISPs. Filtration of route is the setting of route priority and determines which services ISPs can allow to each other. An ISP may have many neighbors but it has peering agreements only with a few of those. Especially with ISPs those have most of the traffic through their neighbors. Filtration prevents false routing updates to other peering and announces only desired prefixes.

Figure 7: Physical Structure

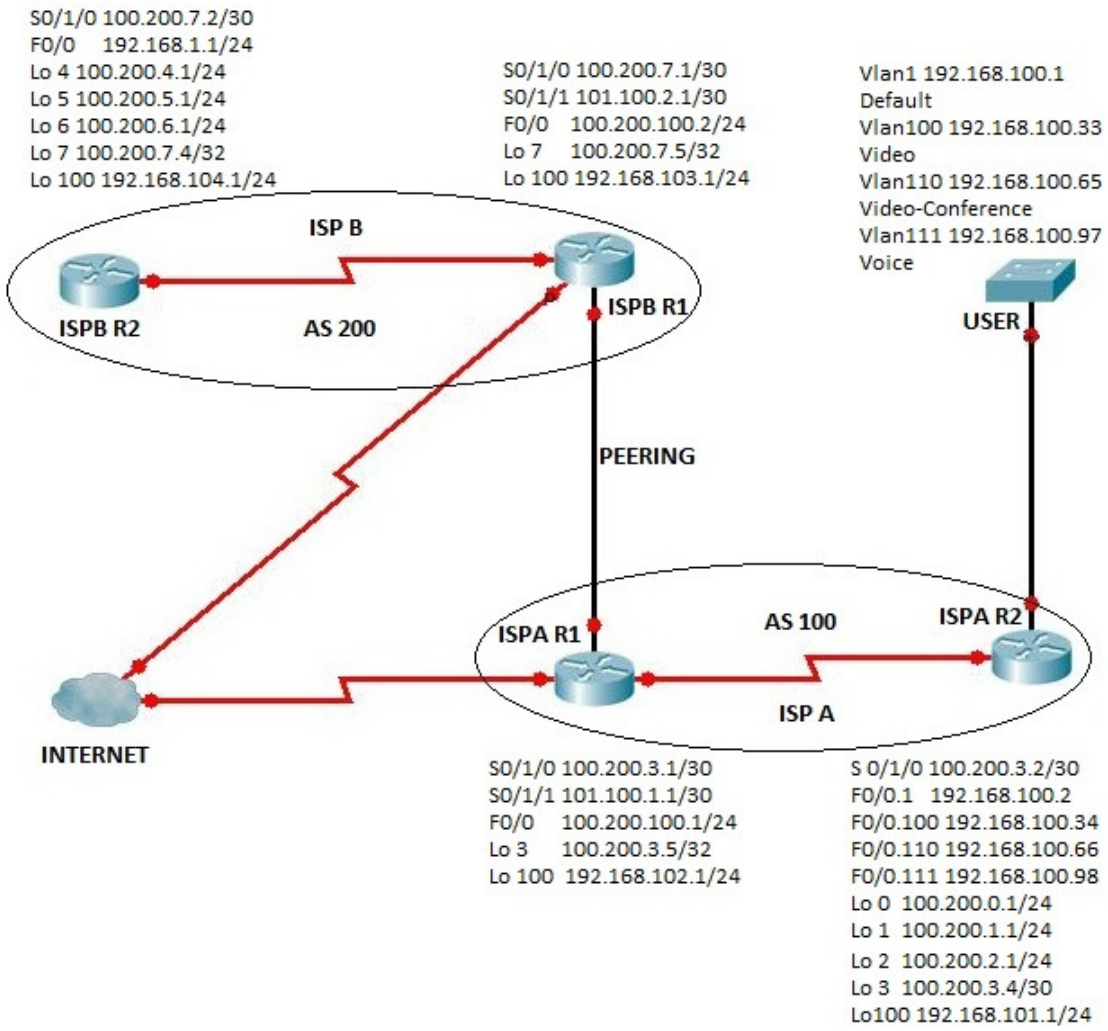


Figure 7 shows the collaboration of ISPs. Connection is through peering and through higher tier ISP or internet backbone.

7.2 Logical Structure

In this scenario, ISP A and ISP B are connected to an Internet exchange point. They also have private peering and are connected through dedicated lines. The ISPs use dedicated lines as a primary link and a link through Internet exchange point as secondary links while providing real time services. The ISPs have two routers in their domains, R1 and R2 respectively. R1 uses EBGP to make peering with other ISPs as exterior and receive all traffic from the internet. R1 in ISPs are responsible for filtering uninterested traffic; it allows interested traffic and passes it on to other BGP neighbors. R1 is responsible for receiving traffic from their customers and advertises customer routes and traffic to other IBGP neighbors as interior and the Internet. ISP A and ISP B use AS numbers 100, 200 respectively. There is a USER connected with ISP A that generates the voice and video traffic and targets communication with ISP B. Different VLANs are configured according to the data servers that are connected to the USER.

ISPs may have two types of customers. single-home customers and multi-home customers. A multi-home customer has two links with two ISPs. Multi-home customers may use both links to send and receive traffic from both ISPs at the same time or use one ISP as a primary link and other link as a secondary link. A multi-home customer is not allowed to provide a transit between ISP A and ISP B. It forwards only directly connected routes to ISP A and ISP B. All loopback addresses simulate single-home customers of ISPs. Each customer of an ISP is assigned 24 network prefixes. A single-home customer can be a corporate customer or local ISP.

ISPs use peering between them to reduce the cost that they are paying for the traffic of their common customers. In this scenario there is a customer connected to ISP A having voice and video traffic. This customer has most of its correspondence with the customers of ISP B. If ISP A and ISP B routes its incoming and outgoing traffic via internet exchange point. Both have to pay for using backbone or services of higher tier ISP. In contrast, if both ISPs agree for peering they do not have to pay to any other party. However, once they use peering, all of the services can be shared between them and it

does not go in the favor of any ISP. So they use prefix lists to limit the uninterested traffic from both sides. These service level agreements vary from ISP to ISP. ISPs may also have an agreement of charges by making a tariff but in most of the cases, peering is done freely.

7.3 Functional Description

ISP collaboration is simple and is the same as internetworking. Where routers are connected by various kind of communication links. They calculate the routes by the information that is Internet based. They receive this information from the hosts on other networks to which they are connected directly and by other routers. An Internet exchange point is a physical place in which Internet connected routers are installed. ISPs that are interested in using the exchange point to get connected to other ISPs. They build links from their routers to the exchange point and connect them to the exchange point routers.

ISPs may communicate in two alternative ways: the first way is the private peering and other way is connection via Internet Exchange Point (IXP). An Internet exchange point is a switching infrastructure that provides services to different service providers to exchange their traffic. ISPs use BGP to facilitate peering with other ISPs. The intention is that both ISPs have a backup link. If a connection fails, ISPs do not lose their connectivity, but establish their connection through the other link. Main ISPs use both private peering, and peering through IXP, to provide better services to smaller ISPs and their customers.

Once the source starts sending a multicast packet. Downstream routers duplicate the packets and flood them to neighbor routers and, ultimately all LAN segments. This is periodic behavior of Cisco's Protocol Independent Multicast (PIM). We work in its Dense Mode. PIM Dense Mode (PIM-DM) uses a simple approach to handle IP multicast routing. In PIM-DM, the multicast packet stream has receivers at most of the locations. An example of our scenario might be a presentation by the CEO of a company as we have used video conferencing. BGP infrastructure is the way to perform inter domain

multicast routing. For the policies where we wanted multicast traffic to flow, the routers had to be multicast capable.

7.4 Internet Protocol Multicast

IP Multicast is a technology for bandwidth conservation that reduces traffic. Its functionality is to deliver a single stream of information to many corporate recipients. We have used it by taking advantage of multicast including videoconferencing and corporate communication. As our goal is to provide real-time services, it delivers source traffic to multiple receivers without adding any additional burden to any end (source end or receiver end) while using the least network bandwidth. Multicast packets are virtualized on the network by PIM enabled Cisco routers. Other supporting multicast protocols, such as we have used BGP, results in the efficient delivery of data to multiple receivers. Another advantage of multicast is that, even if there are thousands of receivers and there are low bandwidth applications, they can get benefit by using IP Multicast. High-bandwidth applications like MPEG video require a large portion of the network bandwidth for a single stream. In this case, the only way to send data to more than one receiver is by using IP Multicast.

7.5 Protocol Independent Multicast

PIM can control despite of the fact which unicast routing protocol has been used to populate the unicast routing table, including BGP, that we have used. PIM uses the unicast routing information to execute the multicast forwarding function. In our scenario, PIM Dense Mode uses a push model to flood multicast the traffic into the entire network. In PIM-DM, routers do not have any downstream neighbors to trim back the unwanted traffic. The flood and trim mechanism is what enables the routers build up their state information by receiving the data stream. Data streams contain the source and group information, so the downstream routers build up their multicast forwarding tables.

7.6 Access Control List

ACLs are commonly used because of its basic capabilities of filtration. They can be configured on all protocols and filter protocols' packets. ACL filtration works as, whether it allows to forward the packet or deny it at router's interface. The criteria is specified by the administrator. This criteria is effective both on the source or destination address of the packets. We have used ACLs in our scenario that permit only IP multicast address 232.0.0.0 0.255.255.255 and deny all other ranges. Because we have to allow only this range for peering purposes. ISP does not want any other service to be shared.

7.7 IP Prefix-Lists

IP prefix lists are also used to permit or deny that are based on prefix matching conditions. These consist of an IP address and a bit mask with an IP prefix-list command. These IP addresses can be a single host route, subnet or class-full network. These lists are used to match the exact prefix range or prefix length. To specify the range of prefix length, le and ge keywords are used. If le and ge keywords are not used the prefix list match the exact. The ge stands for greater and equal. It is used where it assumes the argument to 32 bit length. The le stands for less and equal. It is used where it assumes a lower range than the specified argument.

Prefix lists are configured with a sequence number and/or a name. One of them must be used while configuring this command. A default sequence number of 5 is applied if no sequence number is used that is an increment of 5 for the next prefix list command. If initially a sequence number is entered, the next default will also be the increment of 5. Prefix lists are treated at the start with e sequence number that is the lowest.

7.8 Route Filtration

Filtration is based on autonomous system numbers, prefixes and path attributes. Route filtering can be implemented in four different ways, according to the different precedence order. These are route maps, filter lists, distributed lists and prefix lists. It can be outbound and inbound filtering. For inbound filtering, the order is prefix list, distributed list, filter list and then route map. For outbound filtering the order is filter list, prefix lists, distributed list and then route map. Prefix lists work similarly to access list but are more specific and graceful filtration. Specific ranges are added in prefix lists as predefined private addresses and other ranges have been used for special purposes that are denied, according to the administrative rules.

IP Multicast Range Used in Prefix Lists:

Table 7.1 Usage of IP Multicast range

Starting Range	Ending Range	Usage
224.0.0.0	224.0.0.255	Reserved for well known and special multicast addresses.
224.0.1.0	238.255.255.255	Internet wide and globally scoped multicast addresses.
239.0.0.0	239.255.255.255	Local and administratively scoped multicast addresses.

7.9 Filtration for Special Address

The design demonstrates the working of ISPs in a real time environment of complex peering and transit networks. ISP A and ISP B are the main ISPs. These ISPs may get connected to local ISPs or corporate customers. The ISPs implement IP-Prefix lists of multicast for both customers and neighbor ISPs. The IP prefix list is implemented to deny all inbound malicious traffic on R1 routers of each ISP. Router R1 of each ISP uses an access list to allow only advertisements of its own prefix range. Only the prefixes that match the filtering criteria will be allowed to propagate in the network. ISP A and ISP B use filter-lists and community attributes to stop customers advertising false routing updates. Before establishing neighbor's relationship, ISPs authenticate their EBGP neighbors before creating sessions. A maximum prefix limit is used for each ISP of up to 1000 routes; this can vary according to network requirements. The ISPs cannot send more than a thousand updates to other ISPs. This helps to avoid overflow in routing tables.

Following are some prefixes that are not allowed to communicate because of their special usage. Descriptions are also given.

239.0.0.0 are the addresses that cannot be used for Internet wide or reserved purposes.
224.0.0.0/4 are the addresses that cannot be used as local and administratively scoped.
10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 are the addresses that are used only for local area network purposes.
240.0.0.0/4 are the addresses that are reserved for experiments.
127.0.0.0/8 are the addresses that are used for self testing of the network.
169.254.0.0/16 is the range that is reserved for auto configurations of network interface.
192.42.172.0/24 is that range used at boot process to identify a workstation.
198.18.0.0/15 is the range that is used in testing of devices and benchmarks.
192.0.2.0/24 is the range that is used as example code and documentation.

7.10 Results

The results of this scenario include the investigation to find a solution that combines different methods and configurations to support real-time services when several ISPs cooperate. The other part is demonstration of security solutions in a practical environment. Prefix lists are used to filter private addresses. We have taken some results by generating some malicious traffic of ISP B and interested traffic for the user connected to the ISP A. The prefixes that are added to prefix-list and set to deny, have not been allowed to advertise on these ISPs or the Internet. R1 routers on both ISP A and ISP B deny these addresses. If both ISPs communicate or send updates to each other, these addresses will be allowed to propagate inside the domain. The results are listed below:

Table 7.2 Filtration of Private Address

Local Router IP	Source IP	Prefixes	Action	Method
100.200.3.5	192.68.100.66	172.16.0.0/12	Deny	Prefix list
100.200.3.5	192.68.100.34	100.200.7.4/32	Allow	Customer
100.200.3.5	192.68.100.98	10.0.0.0/8	Deny	Prefix list
100.200.3.5	192.68.100.66	100.200.5.1/24	Allow	Customer
100.200.7.4	192.68.100.34	169.254.0.0/16	Deny	Prefix List
100.200.7.4	192.68.100.66	127.0.0.0/8	Deny	Prefix List
100.200.7.4	192.68.100.98	100.200.6.1/24	Allow	Customer
100.200.7.4	192.68.100.34	100.200.4.1/24	Allow	Customer
100.200.7.4	192.68.100.66	198.18.0.0/15	Deny	Prefix List

7.11 Inspection of Multicast Routing Tables

The “show ip mroute” command has been used for determining the state of multicast sources and groups from the perspective of the selected router.
The output of the command represents a part of the multicast distribution tree with an incoming interface and a list of outgoing interfaces. The output contains a summary that displays a one line summary with the abbreviations of the entries in the IP multicast routing table. It displays statistics about the group and source. It includes the number of packets, average packet size, packets per second and bits per second. It also displays the rate at which active sources are sending the packets to multicast groups. The active sources rate is specified in the kbps and default is 4 kbps.

The output of the “show ip mroute” command is shown in a multicast routing table in a PIM-DM environment:

(*, G) entry, timers, the RP address for the group, and the flags for the group are listed. The incoming interface is the interface toward the RP. If it is null, the router itself is the RP. The reverse path forwarding (RPF) neighbor is the next-hop address toward the RP. If it is 0.0.0.0, this means the router is the RP for the group. The “outgoing interface list” lists the outgoing interfaces, along with modes and timers.

(S, G) entry, timers and flags for the entry are listed. A indicates that it is to be advertised by multicast source discovery protocol. The incoming interface is the interface towards the source S. The RPF neighbor is the next-hop address toward the source. If it is 0.0.0.0, this means the source is directly attached. The “outgoing interface list” lists the outgoing interfaces, in addition to modes and timers.

Table 7.3 IP Multicast Routing Tables

	(*,G) Entry	RP Address	Flag	Incoming Interfaces	Outgoing Interfaces
ISP A R1	(*, 232.32.32.32)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	FastEthernet0/0 Serial0/1/0 Loopback100
	(*, 224.0.1.40)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	FastEthernet0/0 Serial0/1/0 Loopback100
ISP A R2	(*, 232.32.32.32)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 Loopback100
	(*, 224.0.1.40)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 Loopback100
ISP B R1	(*, 232.32.32.32)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 FastEthernet0/0 Loopback100
	(192.168.103.1, 232.32.32.32)	_____	LT	Loopback100, RPF nbr 0.0.0.0	FastEthernet0/0 Serial0/1/0
	(*, 224.0.1.40)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 FastEthernet0/0 Loopback100
ISP B R2	(*, 232.32.32.32)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 Loopback100
	(100.200.7.1, 232.32.32.32)	_____	LT	Serial0/1/0, RPF nbr 0.0.0.0	Loopback100
	(192.168.103.1, 232.32.32.32)	_____	LT	Serial0/1/0, RPF nbr 100.200.7.1	Loopback100
	(*, 224.0.1.40)	RP 0.0.0.0	DCL	Null, RPF nbr 0.0.0.0	Serial0/1/0 Loopback100

Conclusion

The way today's Internet has developed through ISPs' collaboration means that ISPs connect their networks in order to exchange traffic between each other and provide real-time services. ISP interconnection allows traffic of real-time services originating at a source, connected to one ISP's network to reach a destination connected to another ISP's network. These real-time services can be voice and video conferencing. Behind the scenes there lay many individual networks, owned and operated by many different groups, institutional, and governmental entities, joined to each other by interconnection arrangements. Interconnection is the glue that holds the Internet together. The interconnection enables the Internet as a whole to be fully connected. No single network operator could possibly provide internet access in every part of the world. The model on which today's global interconnection arrangements are based has been developing in parallel with the development of the Internet. We have carried out the implementation of a real-time service provision that shows how to configure the ISP interconnection in an operational environment. For this purpose Multicast has been used. This technology offers great advantages to the success of some advanced applications, especially real-time services. Multicast technology is aimed at distributed applications. A few of these advantages are multimedia applications, such as videoconference, that is used in our network in an effective way. Another advantage is, cost of the network resources, the processing in servers and network equipments are reduced. New applications and services can be installed, without the enhancements of network resources and this is economical for the network resources. Multicast reduces the load when using real-time services and there is considerably less possibility for the servers make network susceptible to jams. Implementation design shows a clear picture of the working environment of ISPs. It enables the understanding of the methodology behind the implementation of security parameters. Finally we looked at some tests to check the effects of some major attacks in the operational environment. The results show effective communication with the proper actions that have been taken against attacks.

Sources and References

[1] G. Huston, “Interconnection, peering and settlements,” inet, 1999, available at http://www.isoc.org/inet99/proceedings/1e/1e 1.htm.

[2] W. B. Norton, “Internet service provider and peering,” in NANOG.

[3] T. Roughgarden and E. Tardos, “How bad is selfish routing?” Symposium on Foundations of Computer Science, 2000 IEEE

[4] W. Jiang, D. M. Chiu, and J. C. Lui, “On the interaction of multiple overlay routing,” in Proceeding of PERFORMANCE 2005, Juan-les-Pins, France, Oct. 2005.

[5] Jessie Hui Wang, Dah Ming Chiu, John C.S. Lui, “Modeling the Peering and Routing Tussle between ISPs and P2P Applications” 2006 IEEE.

[6] Lyman Chapin, Chris Owens, “Interconnection and Peering among Internet Service Providers” 2005

[7] J.W. Stewart HI, BGP4: Inter-Domain Routing in the Internet. Addison-Wesley,1998

[8] Y. Rekhter, T. Li, “A Border Gateway Protocol 4 (BGP-4),” RFC 1771, March, 1995

[9] S. Kent, C. Lynn, and K. Seo, “Secure Border Gateway Protocol” to appear in IEEE JSAC.

[10] Matthew Caesar, Jennifer Rexford, “BGP Routing Policies in ISP networks,” Princeton university.

[11] C. Mathew, R. Jennifer, “BGP Routing Policies in ISP Network”, December, 2005 IEEE

[12] Naghlooi Eng, Irdawati Ab Rehman, WaiYang Suit, “An Initial Approach of a Scalable Multicast based Pure Peer to Peer System” 2002 IEEE

[13] Falko Dressler, “How to Measure Reliability and Quality of IP Multicast Services” 2001 IEEE

[14] Panita Pongpaibool, Hyong S. Kim, “Providing end-to-end service level agreements across multiple ISP networks” Carnegie Mellon University, April 2004

[15] Sam C.M. Lee, Joe W.J. Jiang, Dah-Ming Chiu, John C.S. Lui, “Interaction of ISPs: Distributed Resource Allocation and Revenue Maximization” 2008 IEEE

[16] H. Geoff, “The ISP Column”, Internet Society, May 2006

[17] S. Halabi, D. Mcpherson, “The Internet Routing Architectures”, Cisco Press Second Edition, August 23, 2000