Service Provider Networks

Design and Architecture Perspective

First Edition

by Orhan Ergun

Copyright

Orhan Ergun

Chapter 1

Chapter-1 Service Provider Types

{This section is only as a sample and complete part can seen in the Book.}

Transit Service Provider

A company which provides an Internet access to the whole Internet region is considered as a Transit Service Provider. It’s also known as IP Transit Service Provider. Transit is the service of allowing traffic from a network to cross or "transit" the provider's network, usually used to connect a smaller Internet service provider (ISP) to the rest of the Internet.

Figure 1-1 *Transit Service Provider and its connectivities*

In figure 1-1, Provider A is the Transit Provider for Company A, as it also allows Company A to access the entire Internet. In the same figure, Peering connection is shown between Provider A and Provider B. This Peering connection is a Settlement Free Peering which is one of the important Interconnection models and will be explained in detail in this chapter.

{This section is only as a sample and complete part can seen in the Book.}

Content Delivery Networks
Content Delivery Network companies replicate content caches close to large user population. They don't provide Internet access or transit service to the customers or ISPs, but distribute the content of the content providers. Today, many Internet Service Providers started their own CDN business as well. An example is Level 3. Level 3 provides their CDN services from their POP locations which are spread all over the World.
Content distribution networks reduce latency and increase service resilience (Content is replicated to more than one location). More popular contents are cached locally and the least popular ones can be served from the origin.
Before CDNs, the contents were served from the source locations which increased latency, thus reduced throughput. Contents were delivered from the central site. User requests were reaching to the central site where the source was located.
{This section is only as a sample and complete part can seen in the Book.}

Figure 1-4 *Before CDN*
With CDN Technology, the Contents are distributed to the local sites.
Figure 1-5 *After CDN*
{This section is only as a sample and complete part can seen in the Book.}

Chapter 4

Chapter-4 Service Provider Physical Locations

{This section is only as a sample and complete part can seen in the Book.}

POP – Point of Presence

POP is a place where communication services are available to subscribers. Internet Service Providers have multiple POPs in different geographic locations, so subscribers can connect to a location closest to them. POPs can be co-located at the Service Provider's central office (CO). Central Office term is mostly used in U.S and Europe. Access POP is the most commonly used term for the Central Office. Generally, base stations, modems, switches, routers, servers, security and voice appliances are located in the POP sites. POP sites are the demarcation point between customer and Service Provider. POPs can be located at the Internet Exchange Points (IXP will be covered in the Interconnection chapter) as well as the Colocation Centers. POPs can include a meet-me-room which will be explained in this chapter.
Service Providers may classify their POP locations based on speed, hierarchy, technology used in the POP and so on. Earlier it was a trend to classify the POPs with their speeds such as Gigabit POPs, Terabit POPs and so on, but this is not used much

---

anymore. POPs are classified mostly based on their hierarchy such as Access POP, Distribution POP/Aggregation POP and Core/Backbone POP.
Figure 4-2 *Access, Aggregation and Core/Backbone POP*
In each level of hierarchy, users can be terminated but generally the Backbone POP tends not to terminate residential, business or any other types of users.

Also in Access, Distribution and Core/Backbone hierarchy, the Access POP link speed is less than Distribution and the Distribution POP speeds are less than Backbone POPs. In each level of hierarchy, inside the POPs, routers are connected to each other. Access POP's have smaller number of link speeds and also smaller number of routers. Backbone POPs have much higher link speeds and the number of routers are more. Availability and Security of Backbone POPs are also critical.
For the Access and Pre-Aggregation POPs that are connected to different Aggregations POP's, traffic is sent through Core POPs. If the traffic is transferred between two Access POPs which are behind the same Aggregation POP, traffic doesn't go through the Core POP site.
{This section is only as a sample and complete part can seen in the Book.}

Chapter 5

Chapter-5 Service Provider Modules - The Big Picture

{This section is only as a sample and complete part can seen in the Book.}

Introduction

Service Provider's provide many different types of services. Their services are categorized in many different ways.
One way of categorization is based on their customer profile:

- Residential Customers
- Business/Corporate Customers

{This section is only as a sample and complete part can seen in the Book.}

Residential customers are apartments, multi-floor buildings which generally don't require higher speed connections.
Business/Corporate customers are smaller Service Providers, small medium businesses and Enterprises. These customers require higher bandwidth, between 10 Mb to 10s of GB/s.
Another way of categorization is based on the service as well. If end user devices are stationary, the service is called Fixed or wired. If end user devices are not stationary, then the service is called Mobile service. In this chapter, both service categorization (Fixed and Mobile services) and customer profile categorization (Residential and Business Customer service) will be explained.
In Chapter 7 and 8 we will discuss a Fictitious Service Provider Company. In order to understand and create a Service Provider network from scratch, it is important and necessary to understand the Service Provider network environment. Thus, this chapter will cover many different parts of the Service Provider networks. Also, before starting the logical level, protocol and technical discussions about the Service Provider networks, it is necessary to understand each module and the physical layout of the Service Provider's network.
In figure 5-1 (Service Provider Services) , the connectivity , names of the nodes in the specific service, common topologies in each of the services and briefly the Service

Provider networks with sufficient detail is shared. Some operators provide different types of Access connectivity such as Public WIFI, BPL (Broadband Over Power Line), Satellite and also other types of connectivity, but in this book we tried to cover the most commonly deployed Access technologies used in real Service Provider networks. In figure 5-1, there are 12 modules, which are listed as bellow. Each of these modules will be explained in this chapter.

{This section is only as a sample and complete part can seen in the Book.}

---

1. Core/Backbone Network
2. Datacenter and Server Farm Modules
3. Border/IGW Layer
4. XDSL Access
5. FTTX Access
6. Cable Access
7. Mobile Broadband
8. Fixed Broadband Wireless
9. WiMAX
10. National Peering
11. International Peering and Transit
12. Business/Corporate Customers

{This section is only as a sample and complete part can seen in the Book.}

Core Layer Module

The Core layer is the center module of the network, which has the responsibility of connecting all the modules of the Service Provider network together. The traffic between all modules are passed through the SP Core layer. Core/Backbone layer should have high capacity and there is not much protocol, technology and control plane policy found in this layer. It should be designed simple and with high capacity and redundancy.

The Core Layer provides connectivity nearly between each of the Service Provider Modules which are shown in the above list and provides connectivity between different regions of the Service Provider.

Figure 5-2 *Service Provider Network – Core Layer*

The key Characteristics of Core Module are:

▪ High Speed Connectivity.

▪ Bringing Internet Gateway, Access, Aggregation and Datacenter networks together.

▪ Redundancy and high Availability is so important. Redundant physical circuits and devices are very common.

▪ Failure impact is so high in this module, compared to other modules

▪ Full Mesh or Partial Mesh deployment are seen

▪ Commonly known in the Operator community as Backbone or ‘P’ Layer

{This section is only as a sample and complete part can seen in the Book.}

Redundancy in this module is very important. Most of the Core Network deployments in ISP networks are based on Full Mesh or Partial Mesh. The reason of having full mesh physical connectivity in the Core network is that full mesh connectivity provides the most optimal network traffic and the shortest path between the two locations. But not every network can have full mesh architecture, because it is the most expensive design option. Instead, many operators connect their Core/Backbone locations in a partial mesh model. In partial mesh physical connectivity model, all of the core locations are not connected to each other, instead only the Core POP locations which have high network traffic demand are connected together.

{This section is only as a sample and complete part can seen in the Book.}

Border/IGW Module

The Border Module is also called the Internet Gateway (IGW) Module, which hosts Services that will be used before reaching out the Internet. It also provides Internet Access and connects Core/Backbone network to the Internet content.

Services in this module are generally Firewalls, CGNAT, CDN Caches, DNS, Load Balancer, Parental Control boxes and so on. This layer generally runs IBGP with the internal network, and EBGP with other Autonomous Systems.

If residential or corporate customers want to reach the Internet, if content is cached inside the Service Provider, it is served directly from the IGW/Border layer. If the content is not cached in the SP network, then National Peering is checked first.

Content might be found inside the country through the National Peering connectivity.

Inside the country there might be IXP (Internet Exchange Point), which will be explained in detail later in this chapter. In this case, the content is delivered from the IXP in the country through the National peering router that resides in the Border/IGW layer.

{This section is only as a sample and complete part can seen in the Book.}

Figure
5-13
Service Provider Border/IGW Module

{This section is only as a sample and complete part can seen in the Book.}

International Peering and Transit Module

Peering can be done outside of the country as well. In fact, many Service Providers have peering agreement with other companies, both inside and outside the country.

If content is delivered directly from the IXP inside the country, then International bandwidth usage will be reduced. But in some countries, such as very small African countries or Islands, there is no IXP and the only option to reach some contents from the Content Providers such as Netflix, Facebook etc. is receiving the “IP Transit service”.

The “IP Transit service” is receiving the full Internet routing table from another Internet Service Provider. This service can be received within the country or from the International Internet Exchange Points.

For example, Local ISPs in Turkey can receive IP Transit Service (Full Internet Routing Table) from another Local ISP in Turkey, or maybe from an International ISP which has a POP location in Turkey or maybe from an International Transit Internet Service Provider at Amsterdam, London, Germany etc. Receiving an IP Transit Service from different Internet Service Providers will have different impacts. For example, a Tier 2 ISP in Turkey might be selling IP Transit but the overall latency and the quality of routes to the destination will not be the same as receiving the IP Transit from the Tier 1 Operator such as Level 3, Tata etc.

{This section is only as a sample and complete part can seen in the Book.}

Figure 5-24 *International Peering Module*

{This section is only as a sample and complete part can seen in the Book.}

Chapter 6

Chapter-6 Service Provider Interconnections and Peering

Introduction

Peering is a BGP session between two Routers. When different companies have Peering with each other, they exchange network traffic over the peering session. There are three reasons to have BGP peering on Internet:

▪ Company wants to receive an Internet service

▪ Company wants to sell an Internet service

▪ Two companies exchange their customer prefixes and exchange network traffic but don't pay to each other, which is called Settlement Free Peering.

BGP is important, but this is not the topic of this chapter. It is important to understand the business models between the companies on the Internet.

▪ Who peers with whom?

▪ Which company pays to who?

▪ Why they peer or receive a service?

Service Providers sell Internet connectivity. Mostly they purchase Internet service from each other. Enterprises peer with Service Providers as well. From this chapter, you will be able to understand Settlement Free Peering, IP Transit, Paid Peering, Remote Peering and any 'Peering 'related topics. When you finish this chapter, you would not anymore use the term 'Peering' only as BGP neighborship, instead this term will remind you about Settlement Free Peering or Settlement Free Interconnection.

{This section is only as a sample and complete part can seen in the Book.}

Private BGP peering

Private Peering is a direct interconnection between two networks, using a dedicated transport service or fiber. It is also known as bilateral peering in the industry. It may also be called a Private Network Interconnect, or PNI. Inside a datacenter, this is usually a dark-fiber cross-connect. It may also be a Telco-delivered circuit as well. If there is big amount of traffic between two networks, Private Peering makes more sense than Public Peering. Private peering can be setup inside Internet Exchange Points as well.

Larger companies generally use Private Peering rather than Public Peering, since they want to select who they are going to be peer with. Also based on the large amount of traffic that is exchanged between them, they don't want to exchange traffic with everyone by joining the Public Peering.

Public BGP Peering

Typically, Public Peering is done at the Internet Exchange Point. BGP Route Servers are used in Public Peering to improve scalability.

Figure 6-2 *BGP Route Server*

BGP Route Server is used at the Internet Exchange Point to simplify the BGP Peering process. Instead of managing and maintaining hundreds of Peering sessions in large Internet Exchange Points, BGP Route Servers are used. Every BGP speaking router has a BGP session with the BGP Route Server. Route Servers don't change the BGP Attributes, although the type of BGP Peering session is EBGP. The BGP Route Server also doesn't change the next-hop to itself, thus it is used only as a Control Plane device, not a Data Plane. This means that the actual traffic is passed between the companies that participate to the Public Peering Internet Exchange Point.

BGP Route Servers are very similar to BGP Router Reflectors which are used in IBGP topologies. The difference is that BGP Route Server is used in EBGP, but Route Reflectors are used in IBGP.

{This section is only as a sample and complete part can seen in the Book.}

Chapter 7

Chapter-7 ATELCO National Internet Service Provider Design

Introduction

ATELCO is a leading Telecommunication Service Company in Middle East. They have nationwide backbone infrastructure in fictitious country Greenland. They have around 11 million customers in the country; most of them are residential customers. They have Business/Corporate customers from different fields such as other Internet Service Providers, Hosting Providers, Airports, Banks, Hospitals, Holding Companies, Newspapers, Application Providers, Content Providers, Universities, Hypermarkets, Government Companies etc.

{This section is only as a sample and complete part can seen in the Book.}

Regional Connectivities of ATELCO Network

ATELCO's nationwide network consists of 4 regions in the country. They have their POP locations across 60 cities in the country. ATELCO has an international connectivity from each of their 4 regions. Figure 7-1 shows ATELCO's Network

Consisting of 4 Regions.
Figure 7-1 *ATELCO's Network Consisting of 4 Regions*
{This section is only as a sample and complete part can seen in the Book.}

Type-A Cities
This type of city has only Access POP locations. The Access POPs are connected to each other via Ring topology. For connecting the Access POPs to the backbone of the network or connecting to the Internet, these cities are connected to the nearest Type B-City, where there is an Aggregation POP location.
Figure7-*2 (A)* *ATELCO's POP Interconnections – Type A Cities*
{This section is only as a sample and complete part can seen in the Book.}

There are totally 60 cities in ATELCO's network. As it was mentioned above, there are 8 Core POP locations in 4 regions, meaning 2 Core POP sites in each region. ATELCO believes that the Core of the network should be highly available, that's why they deployed all their Core POP locations in different Type-C cities to achieve the most availability as possible.
ATELCO has a total number of 4 Type-C cities around the country that are located in 4 regions. Each region has one Type-C city and each Type-C city has two Core POP sites for redundancy. Core POP locations are connected in a full mesh way. Figure 7-3 shows the Core POP locations in Type-C cities of each region.
Figure7-3 *Two Core POP sites in each region, full-mesh connectivity between Core POP sites*
{This section is only as a sample and complete part can seen in the Book.}

IP/MPLS Multi Service Network
IP/MPLS Multi Service Network consist of Core, Aggregation, Pre-Aggregation and Access networks. ATELCO has many different types of access network connectivity options, providing fixed and mobile broadband connections to their Residential and Business/Corporate customers.
Figure7-*5* *IP/MPLS Multi Service Network – Deployed on Four Regions*
{This section is only as a sample and complete part can seen in the Book.}

ATELCO's Multi Service IP/MPLS network has four layers.
1. Core
2. Aggregation
3. Pre-Aggregation
4. Access Layers

Network devices that form each layer are explained as follow:
▪ P routers form the Core Layer
▪ AGG PE routers form the Aggregation Layer

▪ Pre-AGG PE routers form the Pre-Aggregation Layer and provide connectivity between AGG and Access Layers. The Pre-Aggregation Layer is based on Ring Topology.
▪ AR (Access Router) PE/non-PE devices provide Access Layer connectivity for the different access network types. The access layer physical connectivity for both Mobile and Fixed services is based on ring topology.
Access Layer devices reside in the Access POP locations, Pre-Aggregation Layer routers reside in the Aggregation POP locations and Aggregation and Core Layer devices reside in the Core POP locations.
{This section is only as a sample and complete part can seen in the Book.}

Figure7-6 *Physical POP locations and the layers*
{This section is only as a sample and complete part can seen in the Book.}

Internet Gateway (IGW) and Shared Services Layer

Internet Gateway (IGW) and Shared Services Layer provides Internet Access and connects the IP/MPLS network to the WCL network. All the service nodes, such as Firewalls, CGNAT, CDN Caches, DNS, Load Balancer, and Parental Control boxes and so on reside in this layer. As shown in figure 7-11, this layer runs IBGP with ATELCO's internal network (IP/MPLS Service Layer) and runs EBGP with the Worldwide Connectivity Layer (WCL)

Figure 7-11 *ATELCO's IGW Layer*
For many years, the IGW team were taking care of the Internet service activities inside the country and the WCL team were taking care of all the Internet service activities for outside of the country. These two layers (IGW and WCL) were operated by different teams, but recently they formed a team called AWN (ATELCO Worldwide Network) which will be responsible for ATELCO's worldwide connections.
{This section is only as a sample and complete part can seen in the Book.}

ATELCO's newly formed AWN is taking care of the following activities:
▪ Connection to the Internet Exchange Points
▪ Connectivity with other Operators inside and outside the country
▪ Settlement Free Peering
▪ IP Transit
▪ IRU agreements
▪ WCL Capacity Planning
▪ Service Layer Functions (Parental Control , Firewalls , DNS , Load Balancers , CGNAT deployments)
▪ Service Chaining in the AWN
▪ All BGP (EBGP and IBGP) related activities.
{This section is only as a sample and complete part can seen in the Book.}

Residential Fixed Services

Current Fixed services provided by ATELCO for their residential customers are FTTX and XDSL. Their FTTX design is based on GPON technology. The Current FTTX deployment of the company is purely based on FTTH technology as they think, FTTH is the ultimate goal and will fulfill the ever-increasing bandwidth demand.
As providing DSL services, ATELCO provides ADSL and VDSL services. For the ADSL services, they only provide ADSL v1 .For VDSL services they provide VDSL 1 and VDSL 2 service, which provides much more bandwidth compared to ADSL.
Currently ATELCO has more than 1.6 million FTTH customers coming to their network from all four regions in the country and 2.4 million xDSL customers, so in total 4 million fixed broadband customers which is approximately 20% of the population of the country.
ATELCO has around 400 Access POP locations around the country in four regions and they have their DSLAMs and MSANs for DSL termination devices and OLTs as FTTH gateways in these Access POP locations.

{This section is only as a sample and complete part can seen in the Book.}

Figure7-16 *ATELCO Fixed Residential Service, Access and Pre-AGG rings*

{This section is only as a sample and complete part can seen in the Book.}

Business/Corporate Customers Access Connections

For the Business/Corporate customers, ATELCO has a Metro Ethernet Service which they deploy their switches at the customer location. If multiple companies share the same building, they place larger devices to accommodate more customers.
Buildings are connected to each other in a ring topology. If the capacity requirement is larger in some customer buildings, then the number of nodes in the rings is less. Typically, 6 nodes are used in each business customer ring in ATELCO's network. G.8032 (Ethernet Ring Protection) is used to provide fast convergence in the business customer rings.
These rings are terminated at the Pre-AGG layer in ATELCO's network. At the Pre-AGG layer, if the customer is looking for Layer 2 or Layer 3 VPN service, MPLS starts at the Pre-AGG Layer.

Figure 7-20 *Business/Corporate Customers connection to Pre-AGG Layer*

{This section is only as a sample and complete part can seen in the Book.}

ATELCO IP/MPLS IGP and BGP Design for Mobile Service

OSPF is used in the IP/MPLS network. Different OSPF Process ID's are used between the Access, Pre-AGG and the Core Block (AGG + Core layers). OSPF Router ID is set manually on all the OSPF enabled devices and Loopback 0 IP address will be used as OSPF Router ID on the devices. The CORE network OSPF Process ID is 10.
Fixed and Mobile network devices are only different at the Access Layer. Fixed services devices such as DSLAM, OLT, are terminated at the Fixed Service AR (Access Router), while the Mobile services devices such as CSR (Cell Site Router) are terminated at the Mobile AR (Access Router).
All Pre-Aggregation, Aggregation and Core Layer devices in IP/MPLS network carry

both Mobile and Fixed network service traffic. Core and Aggregation domains are in the same OSPF Process in ATELCO's network.
Figure7-23 *OSPF/MPLS Transport and Inline BGP RR - Mobile Customers*
{This section is only as a sample and complete part can seen in the Book.}

Chapter 8
Chapter-8 ATELCO Network - Design Detail Explanations
{This section is only as a sample and complete part can seen in the Book.}
Figure 8-11 *Content Cache Servers and Transit Operator Connections*

In figure 8-11, ATELCO's users are shown. ATELCO has some Content Providers cache engines inside the network. ATELCO also has Tier 1 Operator connections which have Content Caches in their network too. ATELCO pays Tier 1 Operators to reach the content servers in their network, as well as for the Global Internet.
According to figure 8-11, the Red users (right side of the picture) access the content which is cached inside ATELCO's network. Thus, the Tier 1 Operator network is not used. The Green users (left side of the picture) want to access the content which is not found in the content engines in ATELCO's network, that's why ATELCO sends the user traffic to the upstream network which is its Tier 1 Operator connection. These user's requests are found in the content servers in the Tier 1 Operator which is in the same country. ATELCO still pays for the Tier 1 Operator in this case, but the benefit is lower latency as the content is served from the cache servers within the same country.
{This section is only as a sample and complete part can seen in the Book.}
BGP ORR (Optimal Route Reflection)
Based on this solution, the RR will do the optimal path selection based on each client's point of view. It runs SPF calculation with their clients as the root of the tree and calculates the cost to the BGP next-hop based on this view. So, the Route Reflectors location would be independent from the selection process of the best-path. So, for the same Prefix, each ingress BGP border router can have a different exit point to the transit providers.
Link-state routing protocol is required in the network for the Route Reflectors to have a complete view of the network topology based on the IGP perspective. No changes are required to be done by the clients.
ORR is applicable only when BGP path selection algorithm is based on IGP metric to BGP next hop, so the path will be the lowest metric for getting the Internet traffic out of the network as soon as possible.

This solution is not an alternative to BGP Add-Path or other methods for Path

Diversity, though it is an alternative to provide optimal routing. It can be used together to improve the quality of multiple advertisements, to propagate the route that can be the best path. Also, it can add resiliency and faster re-convergence for the network. For example, by receiving 4 paths from exit point peers across the network, it will choose the best path plus the 3 other paths based on the IGP cost. So, it's a true way to add resiliency through add-path.
With ORR, at the 1st step, the topology data is acquired via ISIS, OSPF, or BGP-LS. The Route Reflector will then have the entire IGP Topology, so it can run its own computations (SPF) with the client as the root. There could be as many rSPFs (Reverse SPF) running based on the number of RR clients, which can increase the CPU load on the RR.
So, a separate RIB for each of the clients/groups of clients is kept by the RR. BGP NLRI and next-hop changes trigger ORR SPF calculations. Based on each next-hop change, the SPF calculation is triggered on the Route Reflector.
The Route Reflectors should have complete IGP view of the network topology for ORR, so a link-state routing protocol is required to be used in the network. OSPF/IS-IS can be used to build the IGP topology information. In the case of single area OSPF area 0, the RR participating in the IGP process has access to the entire LSDB, so it can determine the total IGP costs between each pair of RR-Clients and the IGW (exit points).
{This section is only as a sample and complete part can seen in the Book.}

Figure 8-20 *BGP Optimal Route Reflection (ORR)*
In figure 8-20, without ORR, RR would send IGW3 as the best path to all PE devices, because IGP cost of RR to IGW3 is the shortest path. When ORR is deployed, RR sends IGW1 to PE1, IGW2 to PE2, and IGW3 to PE3 as best paths. This provides optimal routing for each and every RR Client. IGP is great for link state distribution within a routing domain or an autonomous system but for link state distribution across routing domains, EGP is required.
{This section is only as a sample and complete part can seen in the Book.}

Chapter 9
Chapter-9 Evolving Technologies in the Service Provider Networks
{This section is only as a sample and complete part can seen in the Book.}
Egress Peer Engineering
Monetary cost, latency and packet loss are important parameters for the Quality of User Experience for the customers; In the Service Provider networks, traffic engineering can be done by optimizing any of the above parameters.
BGP NLRIs don't provide the information about the cost, latency or loss of the path or exit point for the destinations. In figure 9-5, traditional egress peer engineering and modern way of egress peer engineering are shown. But before that, it is important to explain a specific terminology which is used among the Service Providers. The data-plane interconnection link between different networks is called Network to Network Interconnection (NNI).

Control-plane (EBGP) direct connection between two AS's allows Internet traffic to travel between the two, usually as part of a formal agreement called peering.
This peering can be settlement free based or settlement based (Ex: IP Transit).
Settlement Free Interconnection and IP Transit Connections were explained in the earlier chapters.
The selection of the best exit link for a given destination prefix selection and the enforcement of this selection on a network is not a simple task. This is because the decision for one prefix might impact other traffic by changing the utilization of the NNI link and potentially leading to overload.
Traditionally, SPs use a policy to manipulate the BGP attributes contained in NLRIs received from a peer. This policy-based manipulation is usually performed on the Egress ASBR, but sometimes also on a route reflector (RR) and the Ingress ASBR. This traditional technique provides some level of flexibility and control on how traffic leaves the SP and AS. However, it is also limited by the BGP path selection algorithm and the fact that the results apply to all traffic for given prefix, regardless of the traffic's origin (Doesn't matter which Ingress ASBR sends the traffic).

Figure 9-5 *Traditional Egress Peer Engineering with BGP*
{This section is only as a sample and complete part can seen in the Book.}
Recommended BGP ASN Allocation Schema for 3 Tier CLOS Networks
Figure 9-21 *Recommended BGP ASN Allocation Schema for 3 Tier CLOS Networks*

Recommended BGP ASN Allocation – Using 2 Byte Private ASN

Figure 9-22 *BGP ASN Allocation with 2 Byte Private ASN on 3 stage CLOS topologies*
{This section is only as a sample and complete part can seen in the Book.}
