Taiwan Autonomous System Connectivity Analysis

Grayson Guan

Abstract

The US has long maintained an Internet sanction over Iran. Companies such as Google, apple, and amazon deny Iran access of their tools and services which are vital to modern online communication. However, Iran is able to deal with the situation at a relative low cost for the country's economy by establishing state-based platforms, servers, and data infrastructure [15]. As the tension rise between China and the US in the Taiwan region over the last two year, Internet sanction is likely to happen to Taiwan from either China or the US depending on the Taiwan's stance in the confrontation. In this paper we conducted an Internet route case study for the Taiwan region to gain some insights about ASes in Taiwan. In this study, we developed a general method to acquire ASN and AS-paths in between each pair of ASes in a specific country through data from RIPE. We filtered out the paths which routed outside of Taiwan to determine the country the paths go through. The result also gave insights about the owners of different ASes based on how well they are connected to other ASes.

Keywords— Internet, AS, AS-path,

1 Introduction

The Internet infrastructures are designed to work despite disruption or malfunction of any specific network devices or routers. However, for countries that are heavily dependent on other countries for network traffic routing, the choice of Internet connection is not in their own hands. Even worse, disconnection from another country's networks could results in losing sufficient routing information to reach a number of networks in their country. The disconnection could be for reasons such as natural disasters and or political sanctions.

This project will present an Internet analysis over Taiwan. In the year 2021, the tension between China and US over Taiwan has risen higher than ever. In an article from the New York Times, Evan Medeiros, who served on President Obama's National Security Council, said "The Taiwan issue has ceased to be a sort of narrow, boutique issue, and it's become a central theater — if not the central drama — in U.S.-China strategic competition" [11]. In this project, we aim to answer the following questions, what kind of business could we find through AS network data? What are some reasonable predictions we could make for the owner of ASes based on their routing situation? What country/countries does Taiwan depend on to route from one AS to another?

The rest of this paper is organized as follows. Section 2 discusses the background on AS Border Gate Protocol and BGP looking glass. Section 3 discusses the relevant studies on this subject. Section 4 goes over the data source used for the analysis. Section 5 describes the methodology including data collection and processing. In section 6 the results will be presented and discussed, and address some problems and unresolved issues. Section 7 will display all the data samples mentioned through out the paper.

2 Background

2.1 ISP and Autonomous System

Network attachment points are called IP addresses which are 32-bit (IPv4) or 128-bit (in IPv6) numbers. This format is what makes the Internet's network layers salable. The IP address of an end-host depends on its location in the network topology. This structure allows routes to Internet destinations to be aggregated in the forwarding tables of the routers. For example, any IP address within the range 128.223.0.0/16 in the Internet is in the University of Oregon's (UO's) network, so knowing the 128.223.* is sufficient for any external router to reach UO's network. The structure also allow routes to be summarized and exchanged by routers participating in the Internet routing protocols. Without this aggregation structure, it would be impossible for an algorithm to quickly find a path through millions of hosts connected to the millions of networks belonging to thousands of Internet Service Providers (ISPs).

The term route means the mapping from one IP prefix to another. A router adds this information to its routing table after filtering through all the advertisement options sent by its neighboring routers and then selecting the best route.

Currently the wide-area routing architecture is divided into autonomous systems that exchange readability information [9] through the Border Gateway Protocol (BGP). As shown in Figure.1, an AS is a set of IP prefixes owned and managed by a single commercial organization or entity, and it follows a set of policies for routing packets to the rest of the Internet and exporting routes to other ASes. A unique 16-bit number (aka ASN) identifies each AS.

2.2 Border Gate Protocol(BGP)

Many autonomous systems are Internet Service Providers (ISPs) today, but many are major corporations, colleges, and other organizations that function as their own ISPs. An AS is in charge of both determining how traffic flows inside its own local network and sending data to other independent systems via BGP announced routes. Each AS informs other ASes using BGP about the ASes for whom it will transport traffic. Fig.2 shows AS2 announces to AS3 that it would carry traffic for AS1, AS3 announces to AS4 that it would carry traffic for AS1 via AS2[17].

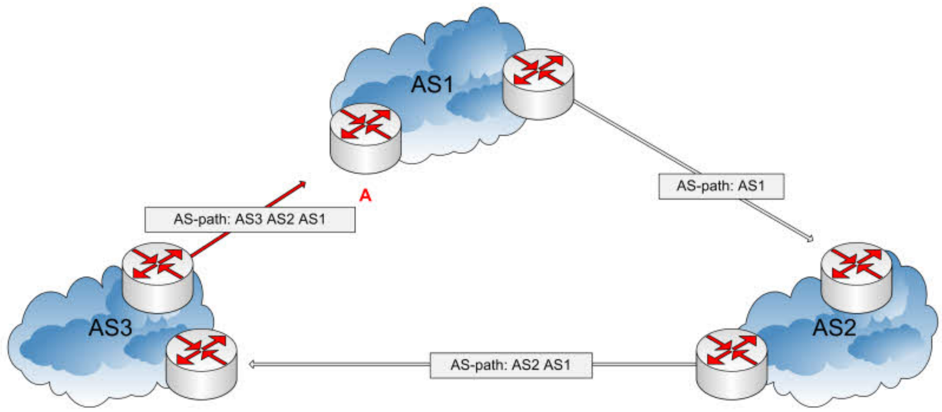

Figure 1: Autonomous systems [13]

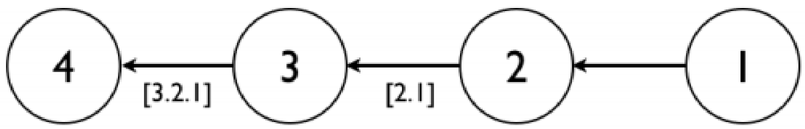

Figure 2: Autonomous systems path announcements [17]

In the example above, for traffic from AS4 to reach AS1, it has to take AS-path [3, 2, 1]. In reality, there are usually multiple paths from one AS to another. The most desirable way for an AS to decide which path to take is through the shortest available path. Whenever the traffic arrives at an AS along the path, the same decision has to be made by this AS as well.

Together, those BGP paths, and ASes make up the AS-level topology of the Internet. One can easily figure out how the traffic is routed through the Internet from point A to point B. However, this information can be used by devious individuals trying to block, servile, or infect the traffic from point A to point B by sabotaging or spying on the ASes in between. From a country's stand point, the AS-level topology provides the necessary information for it to protect or block sensitive information and ensure Internet connection under extreme circumstances such as natural disaster or political conflict.

2.3 BGP Looking Glass

In the global network, Lookng Glass servers collect prefixes from BGP-speaking routers and provide real-time information to network administrators via BGP. They are deployed in different parts of the Internet and provide real-time information about routing and BGP. In the first case, LG helps network administrators troubleshoot, by allowing them to view their prefixes from the "outside". In the second case, Lookng Glass make Internet users understand how BGP speaking routers communicate with Autonomous Systems.

The main purpose for which LG servers are built is to display BGP related information from remote BGP speakers. One example of LG server usage is to check the upstream BGP table after announced prefixes are changed. A network administrator may want to ensure new routes on upstream provider BGP routers are visible after adding new prefixes via a network command. However, the administrator does not have remote access to BGP routers. The administrator can proceed without directs access to the routers by connecting to the provider's Looking Glass server via a web browser and verifying whether the new prefixes are in the BGP table of the provider's routers. To check if the prefixes are not blocked elsewhere on the Internet, the administrator will connect to a different LG server set up for another AS and view the BGP table.

3 Relevant Studies

AS level topology analysis and relationship inferring research have rapidly grown more popular over the last two decades as the Internet grew at a explosive rate. However, country/region studies are relatively rare. [17] outlines a method for mapping national networks of autonomous systems, identifying a limited number of critical autonomous systems that serve as points of control for each national network, and calculating the complexity of autonomous system networks inside each country. [17]'s result have shown that these points of control have the potential to control virtually 90% of the traffic within a given country. [18] developed a country-specific analysis method to scrutinize the inter-domain topology. using both "real world" and "network science" metrics, [18] emphasizes the non-uniformity of interconnections.

[16] established a 'Network-Political Resiliency' (NPR classification) rates a country's political resiliency based on "points of Control(POC)"[17] redundancy level rating, political filtering, total filtering, and Internet Enemies. High NPR score meaning the country's network have low political filtering, and high POC redundancy, which make the networks in the country more resilient to their government.

[10] developed a metric consist of geographic-, technology-, and control-based indices. The result presents a single rank-based score that estimates the Internet resilience of a country compared to others. [10] did extensive work in verifying the geo-location of an AS. Since each AS consist of many IP addresses, it is almost impossible to acquire an accurate location, so the goal is to narrow the location of the AS to a country. [10] combined the data from RIR and MaxMind GeoIP address physical location for each AS. If any IP's physical address is different from the others' within a single AS, then all entries related to that ASN is discarded to avoid ambiguity.

On the other end of the topology analysis is the abstract graph theory centric methods. These methods can be applied to any networks of any kind. On AS-level topology the ASes are the nodes in the graphs. These studies can provide metric to measure the general quality of a network. However, the graph theory model usually down plays the real world AS characteristics such as route and policy originated diversities[18].

Peering is a business relationship which can be established among ASes owners. A good peering relationship can not only save more money for the ISPs but also increase the local connectivity. Including peering relationship information in the analysis can provide additional suggestions for establishing new peering. However, in attempt to infer the peering relationship with BGP data, [18] found that it is not possible to observe and infer all links. In this study, numerous of algorithms for inferring AS relationships produced conflicting results. Additionally, [18] also investigated previous studies on the completeness of observed AS-level Internet and indicate that 10-20% BGP links are missing for Tier-1 ASes and 85% for Tier-2 Ases. The AS-level topology research [8] also revealed that by the time an IXP with over fifty thousands active peering links involving about 400 members is established, the published number of inferred peering links is only reported to be about forty thousand. Prior 2017, this is the main obstacle with adding AS relationship inference into the analysis. [14] proposed a probabilistic algorithm, ProbLink, which resolved the issue of low accuracy AS relationship inference by traditional methods AS-Rank. Jin and his team first identified hard-to-infer links by examining a simple inference algorithm comparable to AS-Rank, and then offered a probabilistic AS relationship inference method that provides a framework for incorporating a large number of noisy but relevant features into the connection inference algorithm. This new Algorithm is more accurate and less sensitive to the locations of vantage points and BGP paths compared to traditional inference program such as AS-Rank[14].

4 Data Source

RIPE NCC (Réseaux IP Européens Network Coordination Centre) is the regional Internet registry (RIR) for Europe, Central Asia, and Russia. This project uses RIPE NCC provided RIPEStat which includes data from various sources including RIPE Database, Routing Information Service (RIS), RIPE Atlas, regional Internet registry (RIR), Blocklists, MaxMind, M-Lab, and Speedchecker [5].

Routing Information Service employs globally distributed set of Remote Route Collectors (RRCs), typically located at Internet Exchange Points (IXPs), to collect and store Internet routing data. Volunteers peer with the RRCs using the BGP protocol and RIS stores the update and withdraw messages. These information are then updated every eight hours[4]. Figure.3 shows the physical locations of all RRCs.

Another available data source for BGP routes is the University of Oregon RouteViews Project. The RouteViews project has route collectors located around the world at key locations(Figure. 4), and more than 260 different organizations share routing information with RouteViews, including some of the largest ISPs in the world [7]. In this project, we used the RIPEStat Looking Glass server. It give users live feedback of the announced BGP routes collected from 23 different available RRCs. It also provides free web API for users to access which is what makes this project possible.

RIR is an organization that oversees the allocation and registration of Internet number resources (such as IP addresses and ASN) in a certain geographic area. RIPE NCC is one of the organizations included since it is a regional Internet registry as mentioned above. The list of RIRs' data provide by RIPEStat also includes AFRINIC (African Network Information Centre), APNIC (Asia Pacific Network Information Centre), ARIN (American Registry for Internet Numbers), and LACNIC(Latin America and Caribbean Network Information Centre)[5].

MaxMind provides geo-location infromation for IP addresses. Considering previous study [10], The RIR geo-location information will only be a temporary solution to locate ASes. Although RIPEStat uses MasMind's data, only ipv4 addresses are available for query. [1] provides API for querying ipv6 and ipv4 geo-locations. An alternative IP geo-location commercial service is IPinfo [6]. IPinfo collects their data using a myriad of techniques and that includes feeds directly with providers (e.g. ISPs, hosting companies, etc), their own sensor network(e.g. ping, traceroute, etc) and various 3rd party sources (e.g. GPS data). As for RIPE Atlas, Blocklists, M-lab, and Speedchecker's data are out of the scope of this project.

"ipinfo" also provides AS ownership information which is very handy when it comes to investigating their backgound. However, since "ipinfo" is a commercial product, they do not provide free API. They advertised using multiple data sources for accuracy, but are unwilling to tell what they are.

Figure 3: Physical location of RIPE NCC Remote Route Collectors[4]

Figure 4: Physical location of Route-Views route collectors.[7]

5 Methodology

Our goal is to investigate the connectivity of autonomous systems (AS) in Taiwan, and map out the autonomous system network. In turn, this will help us find out how much local AS reachability Taiwan will still have in the case it is cut off from the rest of the Internet. To do this we will first need to collect AS-level data including autonomous system number (ASN), ipv4/6 prefix. Next, we can use the RIPE Looking Glass to acquire a snapshot of all AS paths using the ipv4/6 prefix as destination, from here, we can filter out the paths we want. In order to acquire these data, we will use RIPEstat Data API, it is a public data interface for RIPEstat. For each data request, the RIPEstat Data API respond with a json format data file.

First, to get all the ASNs from a specific country, there are two different requests available. The data call "Country Resource List" can lists the Internet resources associated within a country, including ASNs, IPv4 ranges and IPv4/6 CIDR prefixes as shown in the data sample section. To verify if these ASNs are actually active, all ASNs from Taiwan in "ipinfo.io" were verified. The result from “ipinfo.io” showed many of these ASNs are inactive. This can cause slow down in further data collection and statistical calculations.

The alternative data call is “Country ASNs” from RIPEstat. Similar to the call in the previous paragraph, this data call provides information on a country’s registered and routed ASNs, but it separates the inactive ASNs from active ASNs marking them as “non_routed” and “routed” as shown in data sample section. The routing information is based on the data collected with the RIPE NCC’s RIS system. Again the ASNs from this data are also verified through “ipinfo.io”. Second, we can use the ASNs to acquire all the ipv4/6 prefixes under them. The “Routing History” call shows the history of announcements for prefixes. Even though some historical prefixes can belong to other ASNs currently, we can filter out the undesired ASNs at the end.

At this point, the previous query calls can provide us with all the required information in order to use the RIPEstat Looking Glass to look for AS paths for each AS we found in a country. The BGP Looking Glass from RIPEstat uses real time routing data from 23 remote route collectors(rrcs) at different vantage points. In the data sample section, the data “Looking Glass” contains data group “rrcs” lists all paths to the ASN queried detected from different route collectors. This data call provide a near-real-time snapshot of a relatively complete routing view of every ASNs by using the Looking Glass for every IPv4/6 prefix from each ASN. Unlike using traceroute-based tools and Internet Routing Registries, combining the data from multiple vantage points can provide us with a more complete and up-to-date AS topology [12].

Algorithm.1 shows how we conclude if there a domestic route from one AS to another exists. We store all the ASN belonging to the target country in a set (referred to as a domestic ASN set), and all paths in a large dictionary. In this dictionary, each key (representing the target ASN) corresponds to a list of paths which we found through RIPEStat Looking Glass. In order to mark if any path between two ASNs exists within a country, we use a matrix to store the results. I used a matrix to visualize and store the result. The sample table.1 demonstrates how routing information is stored. If there exists at least one domestic path from AS100 to AS200, a “1” is inserted in the table. There exists only (an) external path(s) from AS100 to AS300, so “0” is inserted. There is no path found from AS300 to AS100, so “-1” is inserted. By default, every AS can reach itself, and all entries are initialized to “-1”. To determine if there is any path from any domestic ASN to a target domestic ASN, we will look into the dictionary using the target ASN as key. In this path list, we iterate through each path and check if any ASN in the path belongs to our domestic ASN set. For example, here we will use X as our target ASN, there exists an AS path, [A, B, C, X], and B exists in our domestic ASN set. Then we will check the section from B to X, if C also exists in the domestic ASN set, then we mark the entry from B to X as 1 indicating a domestic path exists. If C does not belong to our domestic set, then we mark the entry from B to X as 0 indicating only an external path exists.

In order to determine which country Taiwan depends on more to route from one AS to another, we have to analyze all unique paths between each pair of ASes in Taiwan. Luckily, we have already acquired the all the paths to reach each AS in Taiwan. Recall the large dictionary

Algorithm 1 AS connectivity

```
country_asn ← set
AS_path ← dictionary
Matrix ← dictionary
for key in AS_path do
    for path in AS_path[key] do
        for asn in path do
            if asn in country_asn then
                for i in path[asn :] do
                    if i not in country_asn then
                        Matrix[asn][i] ← 0
                    end if
                    if i == key then
                        Matrix[asn][i] ← 1
                    end if
                end for
            end if
        end for
    end for
end for
```

we mentioned above, we need to reorganize these paths, and make a new dictionary using each pair of AS as key and store all paths from one local AS to another. Then, the next step is to reduce the paths lists, so that each path in between a pair of AS is unique. For some paths list, just making sure each path is different from one another is not enough, for example, a path like [A, B, B, C] is essentially the same as [A, B, C], since we only care about if the path went through 'B' or not. With that said, each path is also modified, so there is no duplicated AS within the same path. Then for each AS in every path, if they do not exist in our local Taiwan AS set, we can use the "RIR Stats Country" query to determine which country the AS is registered in. We can determine what countries ASes in Taiwan depends to route to one another, and we can compare the number of routes in different countries to determine which country ASes in Taiwan reply on the most.

ASN	AS100	AS200	AS300
AS100	1	1	0
AS200	0	1	0
AS300	-1	-1	1

Table 1: Domestic Path Information Matrix

6 Result

The collection date of the result is 12/05/2021, and Taiwan was used as our study case. The data is only an snapshot of the routing scheme at that specific time. Fig. 5 shows a visualization of Taiwan's inner AS connectivity. On the figure below, yellow, red, and black dots represent domestic, external, and no AS-paths from the ASes on Y-axis to ASes on X-axis. As we can see, there are only limited number of ASes can reach other ASes. This data can give some implication on the ASes from the number of connection they have within the specific region. We used "ipinfo.io" as an additional data source to verify our AS paths and location information. "ipinfo.io" can also help us with identifying the AS ownership and type. However, the "ipinfo.io" API is a paid service, so all of the following investigation from it are done manually.

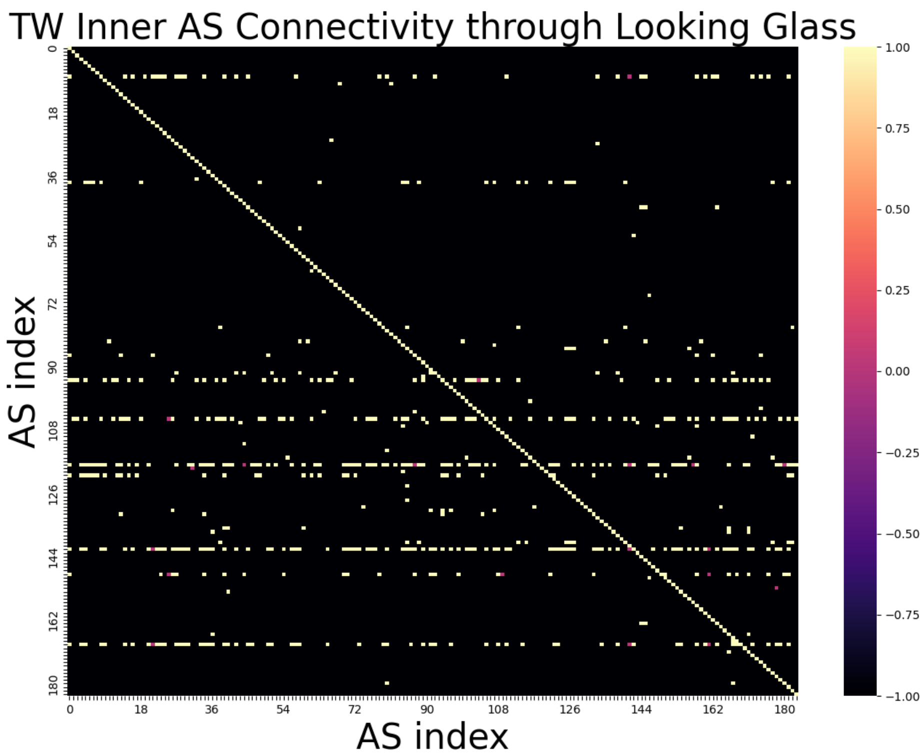

Figure 5: TW AS Connectivity [17]

Diving into more details, our program also gives us text output, showing some statistics of all the ASes through out query and finding out paths as shown in data sample section "Taiwan Connection Report". In all 214 ASNs, we found 34 ASNs that do not have any connection with other local ASNs. Table.2 shows part of our results, we can easily identify some of the largest local isp in the region such as Chunghwa Telecom (AS3462, AS9505, AS9680), Taiwanmobile (AS9924), Far Eas Tone Telecommunications(AS4780), and Chief Telecom (AS17408). In the ASes I investigated, the result shows that AS3462 can reach 92 other local ASes through

Table 2: Taiwan AS Connectivity

ASN	Domestic connection	External connection
3462	92	3
9505	91	5
9924	66	1
9680	63	3
4780	46	1
17408	35	1
...	...	...

Note: This table shows the number of local ASes can be reached by the listed AS through domestic routes and external routes.

domestic AS routes, and 3 ASes through external AS routes. In other words, AS3462 can reach 52.8% of the local ASes, and 96.8% of the routes are domestic routes.

Out of curiosity, I looked into the 3 ASes (AS131605, AS59268, AS38854) which can only be reached by AS3462 through external routes. In the "outbound connection" part of our output, it shows which AS can be reached by AS3462, so it allows us to query all the paths to the any specific target for more information. AS38854 is owned by Zenlayer, an edge cloud services provider based in the United States. All routes connecting to AS38854 from AS3462 has to go through AS21859 which is another Zenlayer AS located in the US, this is also verified through "ipinfo.io" where AS2189 is AS38854's only upstream AS. This makes sense since the company is based in US. AS131605 is owned by INVENTEC BESTA[3], a tech company based in Taiwan. However, the company has many establishments in China as well, this in turn explains in our data why one of the two upstream AS (AS17408, AS138698) of AS131605 is located in China. AS59268 is owned by Qlinks AS which is a United States-based telecommunications company. As we know that AS59268 is registered in Taiwan, but we observed that AS3462 can only connect to it through it's upstream AS139750 located in HongKong, we suspect that Qlinks uses service from "IDCServices"[2] which owns AS139750. So far our data shows that the ASes that are only reachable through external routes all have strong evidence of oversea business connection.

Our result also shows 34 ASNs which do not have any connection with other local ASes. Through "ipinfo.io", their ownership information is also included in the report. Only 5 of them are actually inactive ASes. For the rest of the ASes, there are 21 registered as business, 4 registered as hosting, 2 registered as education, and 2 registered as isp. Similar to the ASes which cannot be reach through local routes from the last paragraph, most of them have strong evidence of oversea business connection. Even though, we cannot observe any connection to these ASes in our current data, that does not mean they cannot be reached by ASes in Taiwan since our method only shows a snapshot of all the AS-path at the instance of query.

Now, if we use the transpose of the matrix we created, for each AS, we can observe the number(range from 1 to 10) of ASes which can reach them. Table.3 shows some of these ASes. AS17415, AS131603, and AS131150 can only be reach by 2 other ASes, of course, one of these 2 ASes is themselves. AS17415 is owned by a small tea company called “Ming Yi Tea Farm”. AS131603 is owned by “World Star” which provides server hosting and server leasing services to small firms and entities. AS131150 is owned by the education Bureau in Kaohsiung City. The pattern here suggest the ASes which can be reach by a small number of other ASes are owned by smaller entities or business. On the other end of the spectrum, we investigated the AS131584 and AS18422 can be reach by 10 other ASes. They are separately owned by “Taiwan Intelligent Fiber Optic Network” and “Industrial Technology Research Institute”. Bothe of these entities are registered as isp, and through “ipinfo.io” and the paths we found, we observed that they both have some of the largest isp ASes we listed above as their upstream (AS3462, AS17408, AS4780, AS9924). So our data suggests, ASes which can be reach by many other ASes are likely to be a smaller ISP.

Table 3: Taiwan AS Connectivity (Inverse)

ASN	Domestic connection	External connection
131584	10	0
18422	10	0
...	...	...
17415	2	0
131603	2	0
131150	2	0

Note: This table shows the number of local ASes can reach the listed AS through domestic routes and external routes.

Another one of our objective is to determine which country does Taiwan depend on to route from one local AS to another. In all 561 pair of ASes which has paths between them, I was able to find 27 pair of ASes uses external routes, and only 17 pairs totally depend on external routes. Table.4 shows in all 39 paths among the 27 pairs of ASes, we found 14 routes go through ASes in China and Hongkong, 11 routes go through ASes in the US, 2 routes go through ASes in the UK, and 1 go through ASes in Malaysia. This result shows that the ASes in Taiwan has a well established local connections, only a very small portion of the BGP routes depend on other countries.

Table 4: External route countries

Country	Number of Routes
China	5
US	11
HK	9
UK	2
Malaysia	1

Note: This table shows the number of BGP routes go through differnt counties in Taiwan

Even though we have figured out the number of routes goes through different countries, to say that ASes in Taiwan depends on China to route just because it has more paths goes through China is not a justified conclusion based on the number of routes. We have to also consider who is the AS we are routing to. One can conclude a route from an ISP to a small business is less important than a route from an ISP to a large business. With that said how would one compare business route to a route connecting to a government network? We have to consider the importance of these external routes with other references such as owner of the AS, size and type of establishment, and the purpose of the AS.

One shortcoming when using looking glass servers to map out AS-paths is that the result we have is only a snapshot of part of all AS-paths available at that time. Although our result cannot give a definitive conclusion on the AS connectivity, it does give valuable insights on ASes we observe. Some of these data collection and analysis method can also be used for other counties. However, the project still have many imperfection such as long run time due to inefficient method of file I/O, and lack of diversity in data source. Another major factor we have to consider is that we have no idea what percentage of the BGP paths are announced to the public. Our result would be a more valuable reference if the percentage is higher.

7 Data Sample

```
Country Resource List
{
    "..."
    "data": {
        "query_time": "2012-12-01T00:00:00",
        "resources": {
            "asn": [
                ...
            ],
            "ipv4": [
                ...
            ],
            "ipv6": [
                ...
            ]
        }
    },
    "..."
}
```

```
Country ASN
{
    "..."
    "data": {
        "countries": [
            {
                "stats": {
                    "registered": 1545,
                    "routed": 1042
                },
                "routed": "{AsnSingle(30720), ...}",
                "non_routed": "{AsnSingle(196613), ...}",
                "resource": "nl"
            }
        ],
        "resource": [
            "nl"
        ],
        "query_time": "2021-11-30T00:00:00",
        "latest_time": "2021-11-30T00:00:00",
```

```
        "lod": [
            "1"
        ]
    },
    "..."
}
```



```
Routing History
{
    "..."
    "data": {
        "by_origin": [
            {
                "origin": "3333",
                "prefixes": [
                    {
                        "prefix": "67.199.138.0/24",
                        "timelines": [
                            {
                                "starttime": "2014-10-13T00:00:0
                                   0",
                                "endtime": "2014-10-24T23:59:59"
                                   ,
                                "full_peers_seeing": 16.25
                            },
                            ...
                        ]
                    },
                    ...
                ]
            }
        ],
        "resource": "3333",
        "query_starttime": "2000-08-01T00:00:00",
        "query_endtime": "2021-12-01T16:00:00",
        "time_granularity": 1036800,
        "latest_max_ff_peers": {
            "v4": 1,
            "v6": 1
        }
    },
    "..."
```

```
}
```

```
Looking Glass
{
    "..."
    "data": {
        "rrcs": [
            {
                "rrc": "RRC00",
                "location": "Amsterdam, Netherlands",
                "peers": [
                    {
                        "asn_origin": "1205",
                        "as_path": "34854 6939 1853 1853 1205",
                        "community": "34854:1000",
                        "last_updated": "2021-11-23T04:37:25",
                        "prefix": "140.78.0.0/16",
                        "peer": "2.56.11.1",
                        "origin": "IGP",
                        "next_hop": "2.56.11.1",
                        "latest_time": "2021-12-05T06:03:56"
                    },
                    ...
                ]
            },
            {
                "rrc": "RRC01",
                "location": "London, United Kingdom",
                "peers": [
                    {
                        "asn_origin": "1205",
                        "as_path": "15692 2914 1764 1853 1205",
                        "community": "...",
                        "last_updated": "2021-10-28T19:10:22",
                        "prefix": "140.78.0.0/16",
                        "peer": "5.57.80.113",
                        "origin": "IGP",
                        "next_hop": "5.57.80.113",
                        "latest_time": "2021-12-05T06:03:57"
                    },
                    ...
                    ]
```

```
            }
        ],
        "query_time": "2021-12-05T06:04:00",
        "..."
    },
    "..."
}
```

```
Country ASN
{
    "data": {
        "countries": [
            {
                "stats": {
                    "registered": 1545,
                    "routed": 1042
                },
                "routed": "{AsnSingle(30720), ...}",
                "non_routed": "{AsnSingle(196613), ...}",
                "resource": "nl"
            }
        ],
        "resource": [
            "nl"
        ],
        "query_time": "2021-11-30T00:00:00",
        "latest_time": "2021-11-30T00:00:00",
        "lod": [
            "1"
        ]
    },
    "..."
}
```

```
Routing History
{
    "..."
    "data": {
        "by_origin": [
            {
                "origin": "3333",
                "prefixes": [
```

```
                    {
                        "prefix": "67.199.138.0/24",
                        "timelines": [
                            {
                                "starttime": "2014-10-13T00:00:00",
                                "endtime": "2014-10-24T23:59:59",
                                "full_peers_seeing": 16.25
                            },
                            ...
                        ]
                    },
                    ...
                ]
            }
        ],
        "resource": "3333",
        "query_starttime": "2000-08-01T00:00:00",
        "query_endtime": "2021-12-01T16:00:00",
        "time_granularity": 1036800,
        "latest_max_ff_peers": {
            "v4": 1,
            "v6": 1
        }
    },
    "..."
}
```

```
RIR Stats Country
{
    "..."
    "data": {
        "located_resources": [
            {
                "resource": "3462",
                "location": "TW"
            }
        ],
        "result_time": "2021-12-28T00:00:00",
        "parameters": {
            "resource": "3462",
```

```
            "query_time": "2021-12-28T00:00:00"
        },
        "earliest_time": "2005-02-18T00:00:00",
        "latest_time": "2021-12-28T00:00:00"
    },
    "..."
}
```


```
Taiwan Connection Report

Query time has been set to the latest time (2021-12-05 00:00 UTC
    ) data is available for.
Total ASN: 214  No connection ASN: 34
No connection ASN:
45599: 141 Yang Guan Jie; hosting (no local or external
    connection)
131631: sunchi networks; business (no local or external
    connection)
131633: sakura internet; business (no path observed, but not
    inactive )
131651: loongaming; isp (no local or external connection)
131662: Denpa Ltd; business (no local or external connection)
131667: GRONEXT CO., LTD; business (no local or external
    connection)
131675: Beyond Orbit Co., Ltd; business (no local or external
    connection)
18043: GETOP Automatic System Inc; business (no local or
    external connection)
139903: RETN Telecoms Ltd; hosting(no local or external
    connection)
140958: Watch Tower Bible and Tract Society of Pennsylvania,
    Taiwan Branch; business (no local or external connection)
211622: TSAI, PANG-WEI; business (no local or external
    connection)
24235: inactive
142005: NC Taiwan Co., Ltd; business (no local or external
    connection)
45761:  Gamania Digital Entertainment Hong Kong Transit AS;
    business (no local or external connection)
135387: Magna Hosting Ltd; hosting (no local or external
    connection)
18178: inactive
```

```
18179: MiTAC Inc; business (no local or external connection)
18186: QianYun Network Service Co., Lt; business (no local or
   external connection)
136462: Mootech Asia; business (no local or external connection)
38187: Gamania Digital Entertainment Co., Ltd;
17717: inactive
17718: Chaijin Information Co., Ltd; business (no local or
   external connection)
139065: Apeiro8 Technology Co., Ltd; business (no local or
   external connection)
138611: Cloud Speed Technology Limited Co; business (no local or
    external connection)
141173: SteveYi Experiment Network; business (no local or
   external connection)
212357: Hung Yun Tseng; business (no local or external
   connection)
135596: Hans Online Services; business (no local or external
   connection)
141742: Magna Hosting Ltd; hosting (no local or external
   connection)
38839: CSPTEK LTD. CO; education (no local or external
   connection)
38845: Fu Jen Catholic University; education (no local or
   external connection)
38846: Wolf Feather Culture Information Co., Ltd; isp (no local
   or external connection)
7649: inactive
210932: Yu-Cheng Kuo; business (no local or external connection)
18428: Mercycat Network; business (no local or external
   connection)

Inner connection stat
length: 132
 Number of connection: 1 : ['...']
length: 23
 Number of connection: 2 : ['9244', '131618', '131634', '131657'
    , '131148', '131677', '24155', '18042', '24235', '9916', '99
    19', '4845', '18178', '18182', '45346', '38187', '17711', '1
    7717', '10135', '24506', '38843', '9678', '7656']
length: 5
 Number of connection: 3 : ['17415', '45250', '38856', '9676', '
    18424']
```

```
length: 5
 Number of connection: 4 : ['131645', '60614', '9416', '212279',
     '7533']
length: 3
 Number of connection: 5 : ['1659', '18185', '7482']
length: 2
 Number of connection: 6 : ['24167', '7481']
length: 1
 Number of connection: 7 : ['7532']
length: 2
 Number of connection: 8 : ['18041', '18046']
length: 1
 Number of connection: 11 : ['134823']
length: 1
 Number of connection: 12 : ['7539']
length: 1
 Number of connection: 23 : ['9264']
length: 1
 Number of connection: 30 : ['10133']
length: 1
 Number of connection: 32 : ['17709']
length: 1
 Number of connection: 35 : ['17408']
length: 1
 Number of connection: 46 : ['4780']
length: 1
 Number of connection: 63 : ['9680']
length: 1
 Number of connection: 66 : ['9924']
length: 1
 Number of connection: 91 : ['9505']
length: 1
 Number of connection: 92 : ['3462']
outbound connection
17408 -> 59268
4780 -> 45250
9924 -> 131610
9505 -> 131642
9505 -> 18046
9505 -> 59268
9505 -> 45504
9505 -> 18424
```

```
45346 -> 133158
3462 -> 131605
3462 -> 59268
3462 -> 38854
10133 -> 131610
10133 -> 139471
10133 -> 38854
24506 -> 10229
9680 -> 131605
9680 -> 59268
9680 -> 38854
outbound connection stat
length: 175
 Number of connection: 0 : [‘...’]
length: 5
 Number of connection: 1 : [‘17408’, ‘4780’, ‘9924’, ‘45346’, ‘24506’]
length: 3
 Number of connection: 3 : [‘3462’, ‘10133’, ‘9680’]
length: 1
 Number of connection: 5 : [‘9505’]
}
```

References

[1] Geoip2 databases demo. https://www.maxmind.com/en/geoip-demo, journal=MaxMind.

[2] idcservices:service. https://www.idcservices.net/services/.

[3] Inventec besta. https://www.besta.com.tw/zh-tw/Page/introduction.

[4] Ripe database. https://www.ripe.net/manage-ips-and-asns/db, journal=RIPE Network Coordination Centre.

[5] Ripestat data sources. https://stat.ripe.net/data-sources, journal=RIPEstat.

[6] The trusted source for ip address data. https://ipinfo.io/.

[7] University of oregon route views project. http://www.routeviews.org/routeviews/, journal=Routeviews.

[8] Bernhard Ager, Nikolaos Chatzis, Anja Feldmann, Nadi Sarrar, Steve Uhlig, and Walter Willinger. Anatomy of a large european ixp. In *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '12, page 163–174, New York, NY, USA, 2012. Association for Computing Machinery.

[9] Hari Balakrishnan. Wide-area internet routing, January 2009.

[10] Annika Baumann and Benjamin Fabian. Towards measuring the geographic and political resilience of the internet. *International Journal of Networking and Virtual Organisations*, 13(4):365–384, 2013.

[11] Chris Buckley and Steven Lee Myers. 'starting a fire': U.s. and china enter dangerous territory over taiwan, Oct 2021.

[12] Hyunseok Chang, Ramesh Govindan, Sugih Jamin, Scott J. Shenker, and Walter Willinger. Towards capturing representative as-level internet topologies. *Comput. Netw.*, 44(6):737–755, April 2004.

[13] Editor. Autonomous system (as), Sep 2019.

[14] Yuchen Jin, Colin Scott, Amogh Dhamdhere, Vasileios Giotsas, Arvind Krishnamurthy, and Scott Shenker. Stable and practical AS relationship inference with problink. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, pages 581–598, Boston, MA, February 2019. USENIX Association.

[15] Mana Mostatabi. The impact of u.s. sanctions on internet access in iran, Aug 2021.

[16] Chloe Reynolds and Saghar Tamaddon. Network-political resiliency. Technical report, Technical Report. Available from: http://www. chloejreynolds. com . . . , 2014.

[17] Hal Roberts, David Larochelle, Rob Faris, and John Palfrey. Mapping local internet control. In *Computer Communications Workshop (Hyannis, CA, 2011), IEEE*, 2011.

[18] Görkem Çakmak and Mehmet Aydin. A country-specific analysis on internet interconnection ecosystems. pages 232–237, 11 2017.