The Art of Peering: The Peering Playbook

<wbn@equinix.com>

Abstract

Several hundred Internet Service Provider (ISP) Peering Coordinators were interviewed over the past few years for the "Interconnection Strategies for ISPs", "Internet Service Providers and Peering", and "A Business Case for Peering" Internet Operations Research papers. In these previous works, we documented the commonly used terminology (Peering, Transit, Transport, etc.), the motivations, the financial justifications and the process of peering.

In this paper we build upon this foundation of peering knowledge and present tactics that Peering Coordinators have used to obtain peering where they otherwise might not have been able to obtain peering. We have identified 19 specific maneuvers that vary from mundane to the clever, from merely deceptive to manipulative. In sum, these tactics represent the "Peering Playbook", the current "Art" of Peering.

Tier 1 vs. Tier 2: Motivations

To understand the tactics employed by ISPs it is important to first understand the motivations of two major classifications of ISPs in the Internet hierarchy.

For the Tier 1 ISPs, there are eight[1] interconnection regions in the United States that make up what is referred to as "The Default Free Zone". In each of these eight interconnection regions, the Tier 1 ISPs[2] connect their networks together in private[3] peering relationships. The motivation for peering is not to reduce transit costs since, by definition, Tier 1 ISPs don't pay for transit. Rather, they seek to minimize their interconnection costs while providing sufficient interconnection bandwidth to support their customer base and their growth. For this reason, the only peering the Tier 1 ISPs need is with each other, and Tier 1 peering policies tend to reflect this.

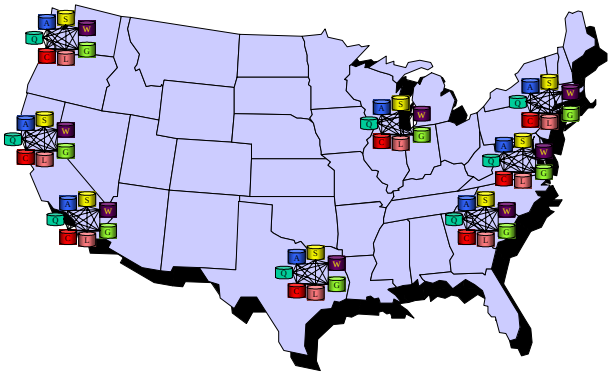


Figure 1 - Eight Interconnection Regions for Tier 1 ISPs

The primary motivations for Tier 2 ISP Peering are to reduce transit fees[4]. Any Internet traffic sent over peering links is traffic that does not go over the comparatively expensive[5] transit links. For like-minded Tier-2 ISPs there is a clear financial win here to peer with each other.

The figure below shows the motivations of Tier 1 and Tier 2 peering players. Thicker arrowed lines reflect greater motivation to peer with the target ISP.

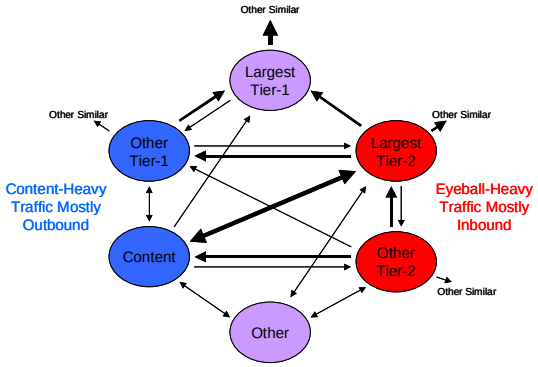


Figure 2 - Peering Motivations: Who wants to peer with whom[6]?

---

[1] NYC Area, Washington DC Area, Atlanta, Chicago, Dallas, Seattle, San Jose (Bay Area), and Los Angeles.

[2] From "Internet Service Providers and Peering", a Tier 1 ISP is defined as an ISP that has access to the global routing table but does not purchase transit from anyone. In other words, the routing table is populated solely from Peering Relationships.

[3] Private Peering is defined as dedicated point-to-point interconnections via fiber, point-to-point circuits, or other non-switched method.

[4] A little bit of an exaggeration here – there are some ISPs that peer primarily for performance improvement. The "Internet Service Providers and Peering" papers highlights these other motivations.

[5] Paul Nguyen (Google) points to the rapidly declining transit prices and relatively static exchange point prices as causing a shift in the motivation for peering from cost savings to performance improvements.

[6] Slide from Gigabit Peering Forum Presentation December, 2001: "New Directions in Peering for Tier-2

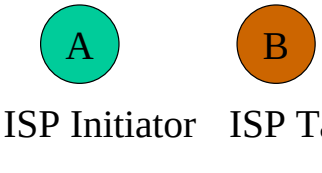
Since the Tier 1 ISPs collectively represent 85% of the routing table[7], they represent the ideal peering candidates for the large Tier 2 ISPs. For a variety of reasons highlighted in the previous research, the Tier 1 ISPs are not as motivated to peer with the non-Tier 1 ISPs[8]. Hence, as shown in Figure 1, the interest in peering is generally one-sided.

Success Stories. The research revealed success stories demonstrating ISPs that started with little or no peering and obtained wide spread peering in a short time period by using one or more of the enumerated tactics. For example, Digital Island Peering Coordinator Mitchell Rose established 50 peering relationships using a variety of tactics described below inside of a year[9]. In two years time, Telia[10] migrated their Internet traffic from 85% transit and 15% peering to 15% transit and 85% peering through aggressively pursuing several of these tactics. Joe McGuckin (Via.net) has emerged with a blended traffic cost of $30/Mbps with a focused 80% peering mix[11].

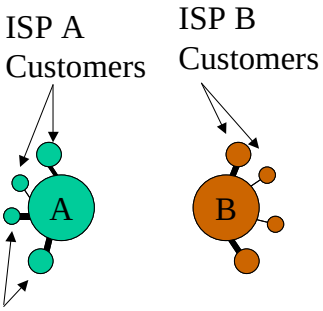
Tactical Peering. This section enumerates 19 tactics that have been used to obtain peering. Where appropriate, we highlight those tactics that are only applicable for obtaining peering with Tier 2 ISPs.

Graphical Representation of Peering

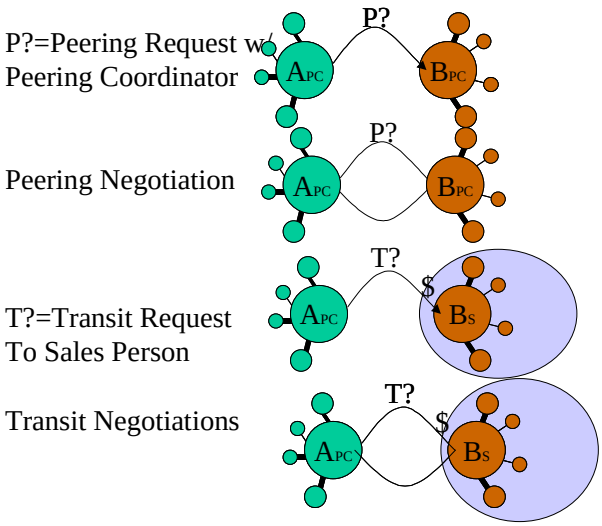
To convey these peering "plays" we will first introduce a graphical language created to describe the maneuvers, starting out with the "ISP Initiator" who is interested in peering with the "ISP Target" as shown below.



The Customers of the Initiator and the Target are shown as same-colored circles attached to the ISP as shown below.



To convey the **Peering[12] and Transit[13] negotiations** process we use the directed arc between the ISPs as shown below. Specific roles are represented using subscript letters. For example, A_{PC} indicates the Peering Coordinator is involved, and B_S refers to a sales person at the Target ISP.



In order to show an **Established Peering Session** we graphically show the transport[14] "pipes" with a 'T' to indicate Transit and a 'P' to indicate Peering. When Transit is shown we place a '$' to indicate who

and Content Providers " , Jeb R. Linton, Staff Network Engineer, EarthLink, jrlinton@ieee.org

7 I don't have a good reference for this but have heard this quote many times. If you know of a reference I'd love to include it here. I know many of the Tier 1 ISPs claim to have 30-40% of the Internet Routes as direct attachments.

8 See "Internet Service Providers and Peering" section called "Reasons NOT to Peer"

9 Conversations with Mitchell Rose (mrose@digisle.net).

10 Conversation with Anne Gibbons (Telia).

11 Conversation at Miami NANOG meeting.

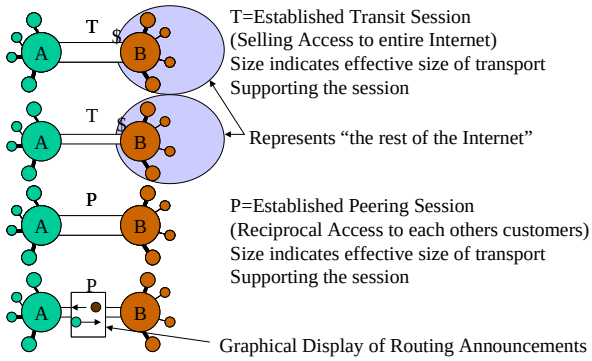
12 Peering is defined as the free and reciprocal exchange of traffic to each others customers.

13 Transit is defined as the sale of access to the global Internet.

14 Data Link Layer connection (i.e. circuits, cross connects, Ethernet MAN, etc.)

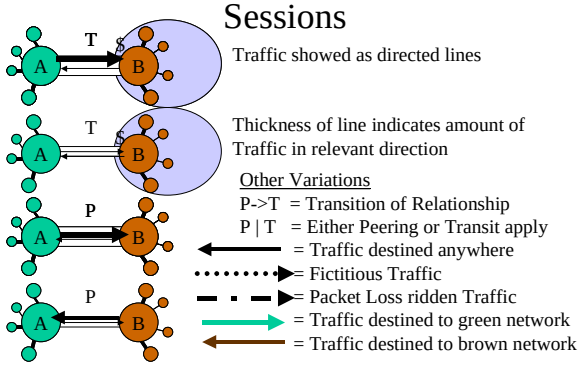
is paying whom for transit. .

Transit and Peering **Sessions**



Finally, to demonstrate **traffic** going over the Peering or Transit pipe, we use directed lines as shown below. When the relevant traffic is destined to a specific network, the directed line is colored to represent traffic destined to the colored ISP. If traffic destination is not relevant, the color black is used. The thickness of the line represents the amount of traffic. Other variations will be presented as they arise during peering plays.

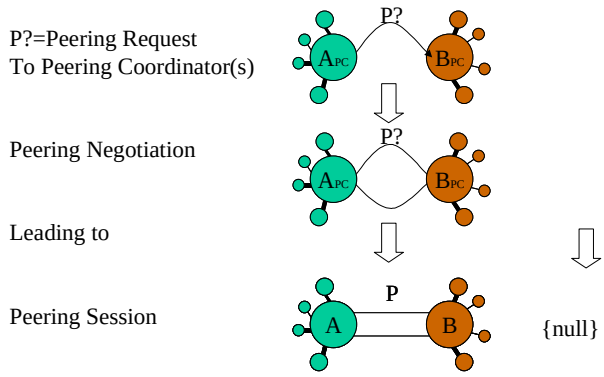
Traffic over Transit and Peering Sessions



1. Direct Approach

By far the simplest approach to obtain peering is to ask for it. Sometimes the response includes a set of peering prerequisites, and, if the prerequisites are met, a follow up discussion with the target ISP to negotiate peering. The "Internet Service Providers and Peering" documents a handful of ways of initiating this interaction.

For each tactic we present in this paper we demonstrate the tactic graphically. The diagrams show the default-free zone at the core, with different colors for each of the Tier 1 ISPs at the core. Around the core (and sometimes interacting with ISPs at the core) are arrows and icons to demonstrate the tactic. For example, in the "Direct Approach", the interactions (shown as arrowed lines) engage the ISP via e-mail, phone calls, etc. directly. Obviously, the more complicated tactics will use these diagrams more fully than in this example.



There are many snafus with the Direct Approach[15]. In many cases the Peering Prerequisites are not publicly available. Many of the ISP Peering Coordinators indicated great difficulty in even getting a return e-mail[16] and/or phone call at all[17]. In some cases it is not clear which peering e-mail address to use[18].

Further, the notion of "Peer" includes the notion of similar size of infrastructure, reach, and traffic volume. The target Peering Coordinator may not know enough about the initiating ISP or may not see the initiating ISP as a true "Peer" and therefore not be motivated to pursue the relationship. Startup ISPs tend to be somewhat optimistic about their traffic

---

15 See "Internet Service Providers and Peering" section called "Reasons NOT to Peer".

16 In several examples, the pseudo-standard peering@<ispdomain>.net bounces. For example: peering@bellsouth.net, peering@verizon.net all bounce today.

17 According to Ren Nowlin (Peering Coordinator from SBC, Carrier 1, and before that Onyx and Level 3) only about 50% of the e-mail sent to peering@<ispdomain>.net get responses.

18 Joe St Sauver (UOregon) points out "Alternatively, going to http://www.google.com/ and typing in:

<provider name> peering or
<provider name> peering contact
AS<provider ASN> peering

often provides amazingly complete results. That strategy suggests, for example (via http://www.pacbell.com/Products_Services/Business/napcontacts/) peering@attglobal.net as an option in the case of ATT..."

growth futures, and since 95% of ISPs use intuition (brand name recognition in many cases) to determine who to peer with, it is difficult for these companies to be seen as a true "peer."

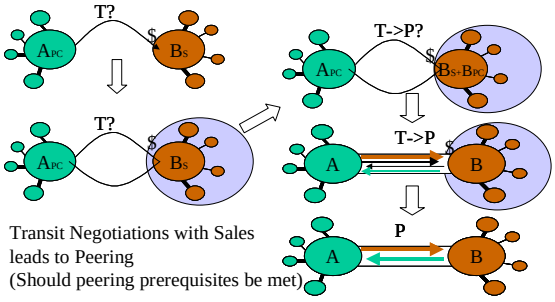
Jeffrey Papen (Yahoo!) claims that persistence pays off with the direct approach. The peering aliases often include a dozen people or more that are not equally vigilant about handling the e-mail. At the same time, anecdotes about expanding the e-mail interactions to include all of peering@<ispdomain>.net have been effective to bring issues to the broader peering community[19] within the target ISP. If discussions get stalled there are additional folks that are up to speed on the interactions. Further discussion pointed to the utility of using a person-to-person contact for discussion to speed things along.

The challenges with the Direct Approach have led Peering Coordinators to employ the remaining additional tactics to obtaining peering.

2. Transit with Peering Migration

"When envoys are sent with compliments in their mouths, it is a sign that the enemy wishes for a truce.[20]"

The Transit with Peering Migration tactic leverages an internal advocate (the target ISP Sales Person) to ultimately obtain peering. In this tactic, a transit contract is *purchased* from the target ISP with an explicit and contractual migration of the relationship from a Transit relationship to a Peering relationship should the Peering Prerequisites at the target ISP be met.

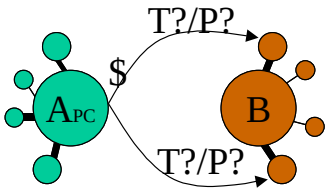


The difficulty with this tactic is that Peering Prerequisites evolve. The challenge here is specifying the Peering Prerequisites to use at the end of the term of the transit contract. In one case study, Williams[21] executed this tactic with Sprint, and by the end of the contract term, the Sprint Peering Prerequisites had changed[22]. Understandably, this led to heated discussions between the parties, and Williams subsequently pursued the "End Run" tactic described next[23].

3. End Run Tactic

"If his forces are united, separate them.[24]"

The End Run Tactic is intended to minimize the need for peering with (and transit through) a target ISP network by aggressively seeking interconnections with the target ISPs largest traffic volume customers (see figure below)[25]. These largest target ISP *customers* are then offered free peering or very low-cost transit services[26]. Those customers that accept these offers reduce the load on transit services and minimize the need to peer with the target ISP.



The difficulty with this approach is that while NetFlow[27] traffic analysis does indicate where the

19 Including the Peering Coordinator's boss!

20 Sun Tzu – The analogy is that the ISP Peering Coordinator offers revenue ("compliments") to the Sales Representative. This is intended as a temporary truce as peering engagements are the ultimate goal.

21 Conversations with Blake Williams (Williams) at the San Jose Gigabit Peering Forum IV.

22 We heard of several cases of this happening with a other ISPs as well. As a result, Transit with Peering Migration is becoming less common.

23 The peering coordinators interviewed observed that the target ISP that fails to transition to peering is very rarely selected for transit.

24 See http://www.online-literature.com/suntzu/artofwar/5/, The Art of War by Sun Tzu

25 Jeffrey Papen's "Tundra" software highlights these potential peers for end run maneuvers.

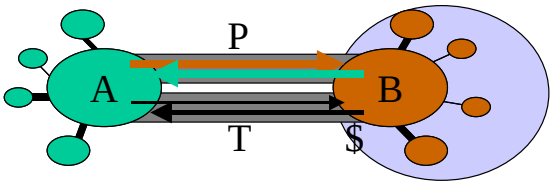
26 In a few cases very low cost was $10/Mbps transit!

27 Cisco traffic analysis engine. Juniper has an equivalent

traffic is flowing and can help prioritize which customers to target, there may be a lengthy and costly sales cycle in order to obtain sufficient traffic volume to reach the desired End-Run goal.

4. Dual Transit/Peering

James Rice (BBC Internet) brought up the Dual Transit/Peering tactic, which is far more common in Europe that in the U.S. This approach combines a transit purchase leverage with a separate peering interconnection. The internal advocate (salesperson) is used to promote the hybrid interconnection approach. This interconnect (shown pictorially below) typically utilizes separate router interface cards and transport to separate customer-customer traffic from transit traffic to make accounting easier. The customer ISP pays for traffic exchanged on the "Transit" interface card and doesn't pay for traffic exchanged on the "Peering" interface card. In some network architectures where peering occurs on "core" routers, this approach may involve separate routers too.

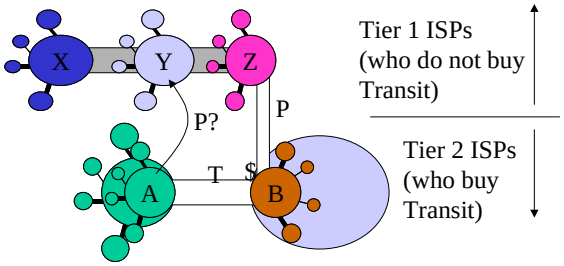


The benefits of this approach include the internal advocate at the target ISP and an architectural cleanness by using separate interface cards. The difficulty with this approach is that some ISPs may not have the internal mechanisms to support this dual interconnection[28], and might rationally prefer a simple transit relationship. Some claim that this has been tried but ultimately gamed to force traffic along the revenue producing path rather than the intended "free peering" path[29].

Note: There is an expression in the Peering Community: "Once a Customer, Never a Peer." Becoming a customer may make you an unacceptable peering candidate[30] so relationships must be timed and managed carefully with potential peers.

5. Purchase Transit Only From Large Tier 2 ISPs

"At first, then, exhibit the coyness of a maiden, until the enemy gives you an opening; afterwards emulate the rapidity of a running hare, and it will be too late for the enemy to oppose you.[31]"



For ISPs just starting out with a desire to become a Tier 1 ISP, the selection of transit supplier(s) is important. Since "Once a Customer, Never a Peer" will prevent peering with Tier 1 ISPs at a future date[32], it is often more cost effective and strategically more effective to purchase transit from a large Tier 2 ISP. As the network traffic grows, and the ISP network expands into peering points, peering can effectively reduce the cost of transit. Once enough peering points are activated, enough traffic is carried, and once the peering prerequisites are met, discussions with the Tier 1 ISPs can begin. Not being a customer of the Tier 1, means that no revenue is lost by peering, and therefore there is one less obstacle to overcome[33].

6. Paid Peering

"Ground on which each side has liberty of

to netflow but both have performance issues. See http://www.cisco.com/warp/public/732/Tech/netflow/ Jeffrey Papen's (jpapen@yahoo-inc.com) TUNDRA software does an excellent job of this type of End-Run analysis. Other commercially available software from IXIA , Adlex and others do the job as well.

28 Paul Nguyen (Google) suggests that a relatively high degree of routing expertise and filtering is needed on both sides to avoid potential routing problems (route disaggregation specifically) with this approach.

29 Anonymous.

30 Even if the potential peer purchases unrelated services, they may still be considered an unacceptable peer.

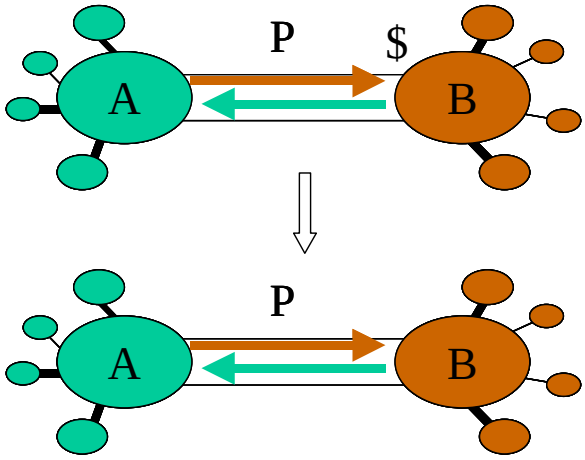
31 http://www.online-literature.com/suntzu/artofwar/17/

32 In one case, a UK based ISP had to turn off transit for over a year before able to engage in peering discussions with its former upstream ISP.

33 A medium sized Tier 2 U.K.–based ISP.

movement is open ground.[34]"

Paid Peering is peering in the usual definition of the word[35] but typically the costs are not symmetric. In some implementations there are traffic-based fees, sometimes based only on traffic asymmetries. Paid peering is sometimes positioned as a stepping stone[36] toward the ultimate goal of free peering between two parties.

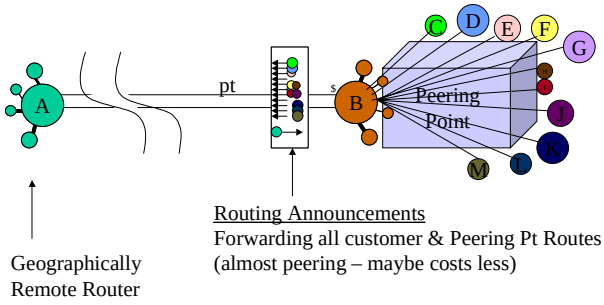


The router configurations, exchange point arrangements, and all peering interconnections logistics can proceed as if they were a free peering arrangement. When both parties agree the peering prerequisites are met, the settlement is no longer implemented and free peering is established.

One form of the "Paid Peering" tactic is where one side covers the cost of the *transport* between the two parties[37]. Covering these expenses may make it easier to overcome objections to peering with early stage ISPs.

7. Partial Transit (Regional)

In this tactic, an ISP[38] sells very low cost transit access to the entire peering population at an exchange point[39] shown as '*x*' in the figure below. This approach is similar to peering at the exchange point without the overhead of buying and deploying additional hardware, and without establishing and maintaining many relationships at an exchange point.



Note that only the routes announced *to* the partial transit provider at the exchange are propagated to the customer. While this is not "Peering" by my definition, it is a useful tactic to quickly obtain exchange point routes and it can be very inexpensive[40] for the Partial Transit provider to provide.

8. Chicken

This confrontational tactic was employed in the late 1990's when Genuity de-peered Exodus. As described in previous work[41], both ISPs exchanged large amounts of peering traffic. Genuity felt it was carrying Exodus traffic "for free" across the U.S. at substantial cost and wanted a more equitable (revenue generating, for example) arrangement. Exodus felt that this traffic was destined across the U.S. but only because Genuity customers desire to access the content. Genuity threatened to de-peer.

---

34 http://www.online-literature.com/suntzu/artofwar/17/ Here the analogy is that both sides can benefit from peering and the give and take is inconsequential, likened to "open ground".

35 Customer-Customer traffic exchange.

36 I first heard about this tactic from Ren Nowlin, then at Carrier 1.

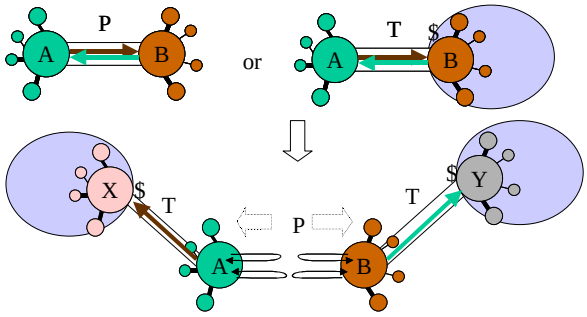
37 Direct Circuits, Local Loops, Exchange Point fees and Cross Connects, etc.

38 A company called Packet Exchange in London now markets this as a standalone service, selling access to routes learned at various exchange points around the world. P.Taylor-Dolan@packetexchange.net

39 James Rice (BBC Internet Service). BBC IS sells partial transit to the members of the LINX that it peers with.

40 The cost of the local loop to the exchange point from the customer is the dominant cost of this approach.

41 The "Internet Service Providers and Peering" paper highlighted the asymmetrical nature of traffic and the clash between these two access-heavy and content-heavy ISPs.



Exodus didn't think Genuity would risk disrupting its customers access to Exodus customers. The end result was de-peering and operational disruptions on both sides. Peering resumed only after both sides reached an agreement to spread the traffic load across more interconnection points across the U.S. to reduce the distance the Exodus traffic was carried on Genuity's infrastructure[42].

The Chicken tactic is employed to abruptly change the peering relationship, and as the case above demonstrates, can have operational impact if neither side succumbs to the change and de-peers. It is worth pointing out that the aggressor of the Chicken Tactic rarely increases revenue from this tactic; the disruption is usually so significant and the destruction of relationship so severe that the "loser[43]" does not choose the aggressor as a supplier of transit services.

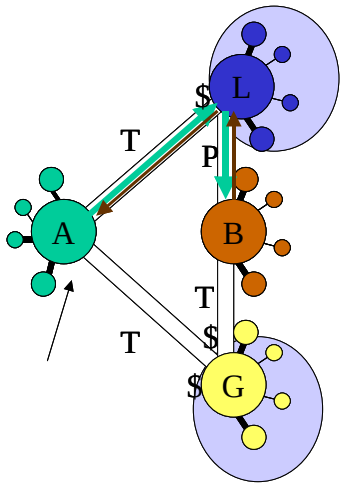
9. Traffic Manipulation: Increase Peer Transit Load

"Startled beasts indicate that a sudden attack is coming.[44]"

One of the more devious of all the tactics presented is the Traffic Manipulation Tactic. To understand this tactic you must recognize that the nature of web traffic is asymmetric, that is, small requests result in large responses. The Content hosters therefore decide which of potentially many paths this relatively large proportion of traffic will flow.

In the Traffic Manipulation tactic, the instigating ISP forces its traffic over the potential peers' *transit* services, to maximize the target ISP's cost of accessing its traffic.

To illustrate, consider the figure below, where ISP A wants to peer with ISP B. Assume that the large responses of content travels through its Transit Provider 'L' to get to requestors on ISP B's network as shown below.



If ISP A asks ISP B to peer, the answer might be "No, we already get your traffic for free through our Peering arrangement with ISP L. So ISP A does not attempt to peer at this point.

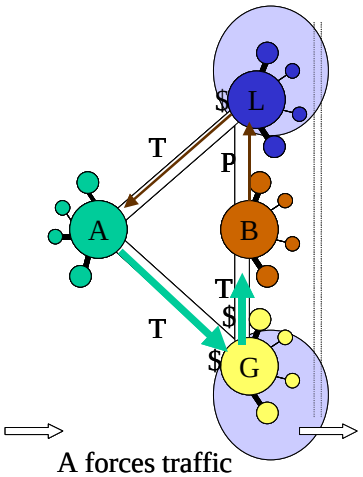
ISP A forces its traffic to ISP B to go through ISP W, which is ISP B's *Transit* Provider as shown below. This causes ISP B's transit bill to increase. I heard stories of how this approach was amplified by using a traffic generator to replay traffic from previous months!

---

[42] Conversations with the parties involved in the conflict.

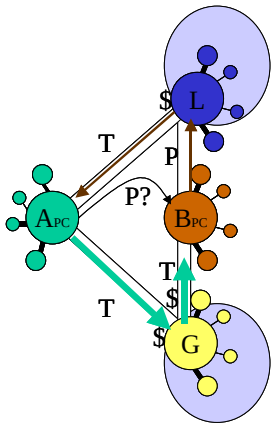
[43] It was also interesting to hear the heated debates over the definition of "loser" in this scenerio.

[44] http://www.online-literature.com/suntzu/artofwar/15/ Lesson #22. The rising of birds in their flight is the sign of an ambuscade. [Chang Yu's explanation is doubtless right: "When birds that are flying along in a straight line suddenly shoot upwards, it means that soldiers are in ambush at the spot beneath."] Startled beasts indicate that a sudden attack is coming. Our analogy here is that the traffic influx may be the traffic manipulation tactic.



A forces traffic
Over B's transit

After some time elapsed, ISP A opens a dialog with ISP B, who reviews the traffic analysis data and is surprised that ISP A has not appeared on the radar screen as a potential peer. Seeing the great transit expense that is paid for access to this traffic, the peering decision is easy for ISP B; ISP A is clearly a large traffic peer that is expensive to access over a transit link. Peering is established with the target.

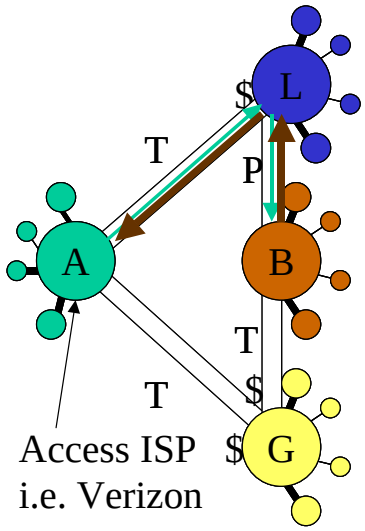


1 MONTH LATER
Contact PC-We should Peer!

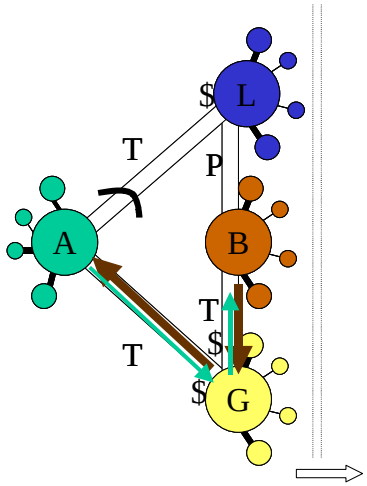
Traffic manipulation stops[45] about a month after peering is established. Since only a very small percentage of ISPs do the traffic analysis[46] necessary to detect this maneuver, this tactic often goes undetected.

The Traffic Manipulation Tactic is most effectively deployed by network savvy Content Providers. Since web traffic is asymmetric, the producer of the responses (the content player) has the greater ability to force a larger amount of traffic along one path or another.

Access Heavy ISPs play this game as well but with different techniques. The initial state is the reverse of the Content Heavy scenerio described before; small requests generate large responses from the content provider.



From my conversations I heard of two tactics to force traffic to go along the path that costs the target ISP the most money to access the access providers. The first technique is to simply stop announcing its routes to the target's Peer. This forces all traffic to use the alternative path, resulting in increased transit fees for the target ISP.



A forces traffic
Over B's transit

45 Anonymous. Multiple Content Companies have admitted to this maneuver.

46 "Internet Service Providers and Peering" research showed that fewer than 5% of ISPs have the resources for traffic analysis.

The second method I discovered was that ISP A would prepend the AS for ISP B into its route announcement. This way, when BGP propagates the routing information to ISP B, the BGP code would see a routing loop and invalidate its route to A along this path. This tactic is seen in the community as "evil, clever, and anti-social" at the same time.

A few additional notes from the Peering Coordinator Community. First, this tactic requires a large amount of spare capacity to handle the manipulated traffic to go along alternative path[47]. Second, if the tactic is detected, the Peering Coordinator Community is small enough that everyone in the community hears about it. At the same time, Traffic Manipulation is used by some ISPs as a way to manage Traffic Volume Ratio requirements for peering with the Tier 1 ISPs.

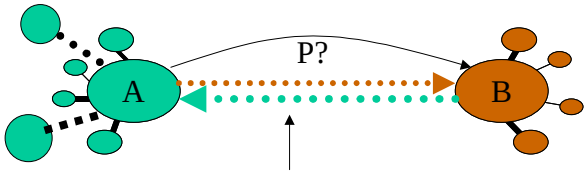
As stated above, one amplification tactic of the Traffic Manipulation approach is to add traffic generation to the mix[48]. Some ISPs would replay traffic in increasing multiples of Megabits per second in order to meet peering traffic minimums and/or meet traffic ratios[49].

10. Bluff (Traffic Load Futures or Performance Problems)

"All warfare is based on deception.[50]"

This tactic refers to the game of Poker where one player over signals its strength, or bluffs. Specifically, peering prerequisites often include traffic volume minimums to be met in multiple geographically distributed locations. Since many Peering Coordinators do not do the required traffic analysis to disprove an assertion[51], and the cost of being wrong could be an expensive transit bill, the assertion may be accepted as truth.

Traffic Load Futures. The Peering Coordinator in this maneuver typically asserts that the required traffic volumes for peering a) are met today, or b) will be met at some point in the future based upon some event. A large customer[52] soon to be installed is a common form of bluff.



This approach is effective for several reasons:

1) It is difficult for the target ISP to determine how much traffic will be exchanged if a peering session is established[53],
2) It is more difficult to determine if the initiating ISP is bluffing with respect to the new customer win(s),
3) It is more difficult still to project the resulting traffic volume should the customer installs go forward.

In summary, if the initiating ISP is NOT bluffing, it is difficult to compare the transit cost increase to the incremental load on the targeted ISP infrastructure. Since transit is generally an order of magnitude more expensive than peering[54], if there is a chance the initiating ISP is not bluffing, peering generally makes sense. As with Poker, once the bluff is called and found to be false, future peering negotiations and claims may be difficult.

Performance Problems. Eric Anderson (BT Ignite) mentioned a slightly different but related bluff. An ISP Peering Coordinator can also be motivated to peer if the other party can demonstrate a significant performance problem that can be solved by peering. Since both ISPs have customers that are suffering from packet loss for example, both parties have some motivation to fix the problem.

---

47 Anonymous.

48 Conversation with James Spencely at APRICOT 2002 in Bangkok.

49 Some ISPs will peer only to the extent that the inbound and outbound traffic is relatively even, or meets a particular traffic ratio.

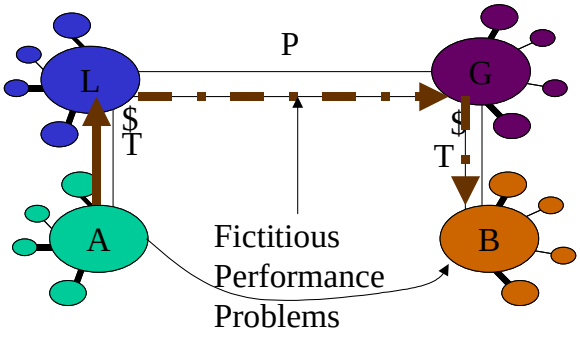
50 Sun Tzu – Tier 1 ISPs often have a "Peering Steering Committee" to evaluate peering requests.

51 Previous research shows that less than 1 in 20 ISPs do the required traffic analysis to prove or disprove these assertions. See "Internet Service Providers and Peering" for data points.

52 "We have Hotmail and Microsoft coming on as a customer" seems to be the most common form of bluff.

53 According to Sean Donelan, even the Tier 1 ISPs do not have the resources to determine if peering candidates meet their traffic volume peering prerequisites.

54 See "A Business Case for Peering". Send e-mail wbn@equinix.com to obtain any of these white papers.

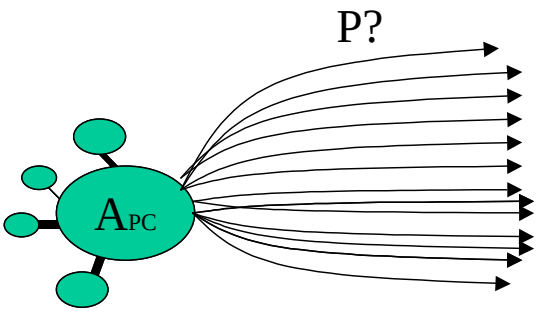


Since few ISPs actively perform the network traffic measurements, they can be persuaded of network problems where none exist. In one case, the evidence of poor performance was a series of traceroutes to demonstrate the packet loss and latency associated with traffic between the two route. By verifying with tools such as Looking Glass these traceroutes were determined to be a farce and peering was not established.

These two tactics generally apply to Tier 2 ISPs peering with other Tier 2 ISPs or content players. There was significant debate in the community about the effectiveness of this tactic[55].

11. Wide Scale Open Peering Policy

"65. If the enemy leaves a door open, you must rush in.[56]"



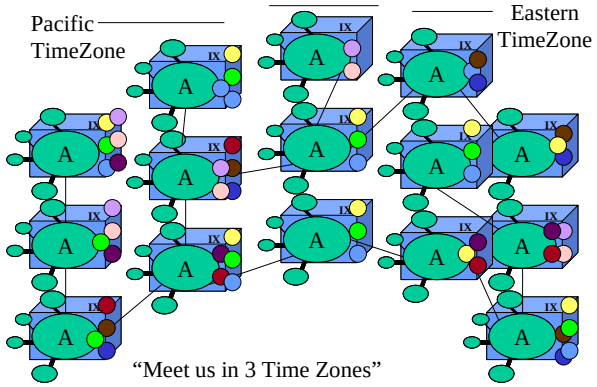
One tactic to obtain peering is to publicly promote an open peering policy to the Peering Coordinator community[57].

Peering Coordinators face rejection and having phone calls and e-mail messages go unanswered as a part of their job. Finding an ISP that has an open peering policy typically means that there will be little resistance in getting peering established. Since the number of peering sessions and the amount of traffic exchanged in peering relationships is often used to gauge the effectiveness of a Peering Coordinator, obtaining peering with "Open Peering ISPs[58]" is an easy way to make the Peering Coordinator look good.

The Wide Scale Open Peering Policy tactic is an untargeted approach and generally is executed only by Tier 2 ISPs looking to minimize their transit costs by maximizing their peering with other small and medium sized ISPs.

12. Massive Colo Build

Along the same lines but separable from the Wide Scale Open Peering Policy is the tactic of building a large number of Points-Of-Presences (POPs) in a large number of exchange points[59]. This tactic maximizes the possibility of meeting the collocation peering prerequisite with a large number of target ISPs in geographically dispersed locations.



13. Aggressive Traffic Buildup

"Forestall your opponent by seizing what he holds dear, and subtly contrive to time his arrival on the ground.[60]"

The Aggressive Traffic Build up tactic involves acquiring a massive amount of customer traffic that an ISP can then turn around and offer to a peer by peering arrangement. Since the alternative way to access this traffic is through expensive transit

---

55 Seasoned Peering Coordinators claim that this tactic is so common that it is not taken seriously anymore.

56 http://www.online-literature.com/suntzu/artofwar/17/

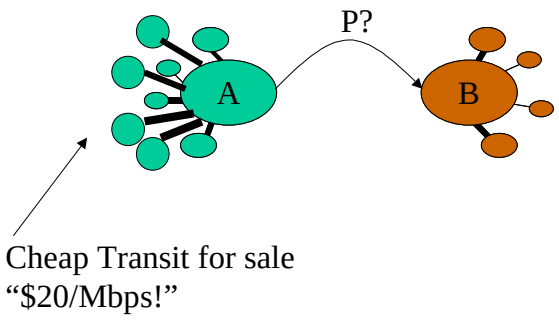
57 AboveNet, Akamai, and many other Open Peering Policy ISPs do this very publicly.

58 See Appendix A for a list of known "open" peers.

59 Cogent, SBC, Adelphia are all examples of ISPs installed at a large number of exchange points.

60 Sun Tzu, The Art of War. Online: http://www.online-literature.com/suntzu/artofwar/17/

relationship(s), the target ISP is motivated to peer.



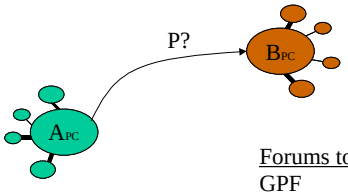
To obtain massive amounts of customer traffic, the ISP offers ultra-low-cost transit and/or strategic relationships to sell VPNs, Intranets, high bandwidth video, and even traditional carrier services over existing Internet infrastructure.

This tactic is only applicable to Tier 2 ISPs[61]. It is also a way for the Tier 2 ISP to ultimately meet the traffic volume prerequisites for peering with the larger players. Care must be taken with this tactic in order to balance peering traffic ratios[62] at the same time as picking up massive amounts of traffic[63].

14. Friendship-based Peering

"On the ground of intersecting highways, join hands with your allies. [Or perhaps, "form alliances with neighboring states."[64]]

It is often said that peering is a game of relationships, and this tactic simply makes that point. Peering relationships have been established between networks of unequal size solely based upon friendships between Peering Coordinators have with one another[65]. Attending NANOG, hiring Peering Coordinators with many years of experience, and leveraging introductions[66] are all ways to build relationships.



Forums to meet Peering Coordinators
GPF
NANOG
APRICOT
RIPE
IETF
:

Some exchange points have established a role of "Peering Facilitator" that pulls together the Peering Coordinator community. This has been especially effective at International Exchange Points where the participants may come in from different countries and may not know each other[67].

To avoid regulation[68] most of the Tier 1 ISPs have stringent peering request process that would not allow a casual peering session to be established. For this reason, this tactic only applies to Tier 2 ISPs.

15. Spam Peering Requests

One approach Mitchell Rose (Digital Island) used to establish peering was to send e-mail non-selectively to all participants at various exchange points. Please make sure that "Reply to Self" and not "Reply to List" is selected[69]. This approach led to dozens of peering sessions very quickly. Since many exchange point participants adopt the Peer Widely and Peer Openly tactic, this approach effectively yields peering with a potentially large number of ISPs and Content companies.

---

61 Since the motivation is to reduce transit fees to peer, and the initiating ISP has a lot of traffic to offer. As before, since Tier 1 ISPs don't pay transit fees, this approach doesn't apply.

62 Jeb Linton, Earthlink.

63 Joe Klein (Adelphia)

64 http://www.online-literature.com/suntzu/artofwar/17/

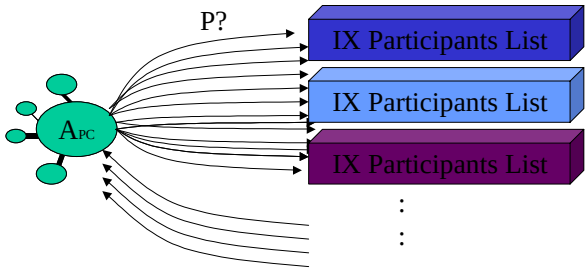
65 Conversations with Vab Goel, former lead engineer from Sprint and Qwest.

66 The Author has helped the Peering Coordinator community through introductions at NANOG, IETF, RIPE, and APRICOT meetings. This has led to dozens of peering sessions!

67 Josh Horn (Terramark, NAP of the Americas) helps with the introduction and education aspects of this job for the NAP of the Americas (NOTA) with the population from South America.

68 Peering is unregulated and Tier 1 ISPs want to keep it that way.

69 Plea from Stephen Stuart (MFN)



The problem with this approach is that the result might be a large number of high maintenance low volume peers. This tactic is generally only employed to Tier 2 ISPs; Tier 1 ISPs have plenty of large volume peering candidates approaching them so they don't generally solicit peering.

16. Honey Approach

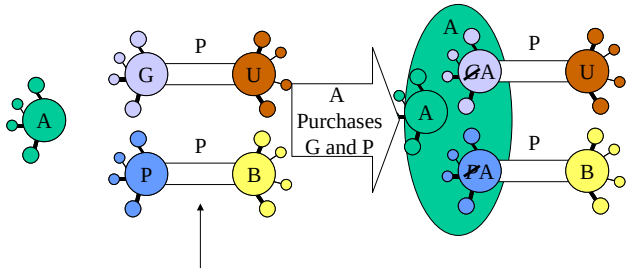
"Begin by seizing something which your opponent holds dear; then he will be amenable to your will.[70]"

Named for the adage[71], Yahoo! adapted the Honey approach by promoting the desirability of its content as a key reason to peer with them. As one of the largest portals in the world, Yahoo! describes the thousands of live webcast events, the hundreds of thousands of concurrent streams of content delivered, the gigabits-per-second of raw traffic flows, etc. as reasons why an ISP should want to receive that over a peering relationship instead of through their transit relationship. Since ISPs hold their network performance dearly, Yahoo! leverages this performance aspect lure well.

This tactic is only applicable for content heavy Tier 2 ISPs and network savvy content players.

17. Purchase Legacy Peering

This tactic was more popular in the 1990's than it is today, but it is worth noting. Level 3 was unable to obtain peering with the Tier 1 ISPs in the early days so it acquired networks[72] that had already established peering with a couple Tier 1 networks. Under the assumption that this peering would transfer to the larger aggregate company, Level 3 acquired the ISP in order to leverage the pre-established peering arrangement[73] and build upon it.

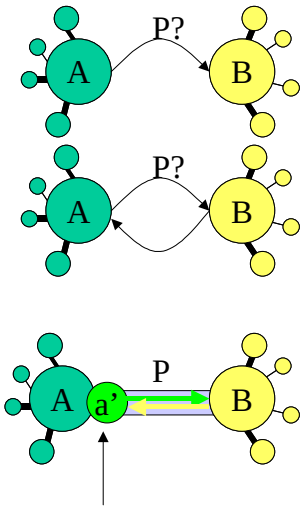


Some would say that this is the easiest tactic[74] to execute, but some caution legal review of the Peering Contracts, and warn that most peering contracts (BiLateral Peering Agreements) have 30 day termination clauses.

17. Bait and Switch Tactic

"Hold out baits to entice the enemy. Feign disorder, and crush him."

A large parent company may be able to initiate peering negotiations where a smaller subsidiary may not. The Bait and Switch tactic leverages this fact by negotiating peering for a large traffic source or sink, and then announcing a different and much smaller traffic source or sink when setting up peering.



18. False Peering Outage Tactic

---

70 Item 18. If asked how to cope with a great host of the enemy in orderly array and on the point of marching to the attack, I should say: "Begin by seizing something which your opponent holds dear; then he will be amenable to your will." Sun Tzu http://www.online-literature.com/suntzu/artofwar/17/ .

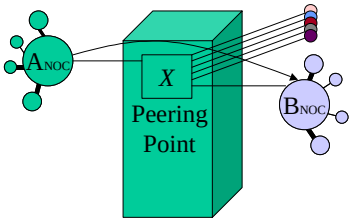
71 The old adage, "You will attract more bees with honey than with vinegar."

72 Level 3 buys Geonet. Other examples include: Cogent buys NetRail, Aleron buys Telia/AGIS, Cogent buys PSINet assets.

73 Anonymous.

74 Joe Klein (Adelphia, formerly Cogent)

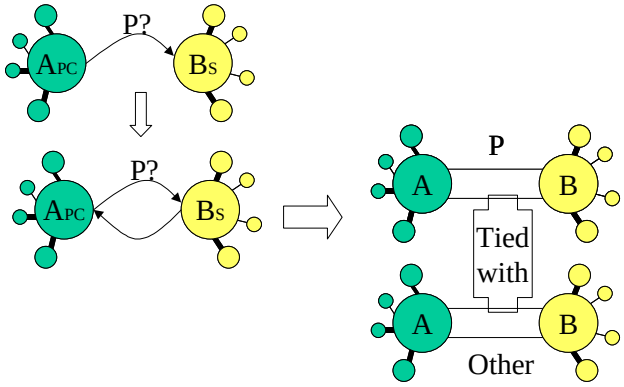
To set up this tactic, both ISPs attach to a shared exchange point fabric such as an Ethernet LAN. The target ISP network operations center is then contacted to "repair" a down peering interconnection. The target NOC and/or on-call engineer may edit the router configuration and establish peering where peering was never intended to be established[75].



ANOC: Hey – Emergency!
ANOC: Our Peering Session with you Went Down!
BNOC: Strange. <looks on router> I don't see it configured.
ANOC: It was. Don't make me escalate to <famous person>
BNOC: Ah – I bet is was that last config run that trashed it.
BNOC: Give me a few minutes to fix it on both ends.

19. Leverage Broader Business Arrangement

One large ISP met the peering prerequisites of a Tier-1 ISP but was refused peering because peering would significantly reduce transit revenue[76]. The objection was overcome by expanding the broader business relationships in exchange for peering. The resulting combined arrangements left the Tier 1 cash flow neutral or slightly cash flow positive and with a stronger customer relationship by selling its other services.



Another example: "Say you have both an ISP side and a Telco side. If some other ISP comes to your telco side wanting to buy services, include in the contract that they must peer with your ISP side[77]."

What Doesn't Work

"To begin by bluster, but afterwards to take fright at the enemy's numbers, shows a supreme lack of intelligence."

Conversations with Peering Coordinators revealed several approaches that were not effective.

1) Foreign PTTs have attempted exert market dominance in a new market as if they were the PTT in the new market. Attempting to leverage power position in a foreign land in a new market has proven ineffective.

2) Threatening litigation and government intervention often shuts down the conversation between Peering Coordinators.

Note: I received pushback from several ISPs on this item – several said that applying regulatory pressure has been effective. For example, during pending mergers (e.g. WorldCom and Sprint) some ISPs used peering in trade for not claiming monopoly powers of the merged entity.

3) Public Name Calling and badgering in public forums proves to bring personality conflicts into play and often results in doors being closed that should be open.

4) Make sure you research peering requirements and your people network well before initiating contact. Many peers insist upon geographic diversity for peering.

5) Demonstrating lack of knowledge regarding backbone operations often stops the peering discussion. Interestingly, demonstrating too much knowledge was cited when arrogance led to personality conflicts. "In the end it's knowledge and Attitude.[78]"

6) Refusal to register routing information in the Routing Registries is a quick way to have peering requests ignored.

---

75 Chris Cousins (Carrier1) and several others reported having seen this attempted. One other reviewer anonymously acknowledged that this has resulted in peering.

76 It is rare that this truth is revealed. More often excuses are given such as lack of bandwidth for additional peering traffic, interface card shortage, contractual reviews, etc.

77 Contributed by Andrew Partan, e-mail April 8, 2002

78 William F. Maton, e-mail regarding the draft.

Summary

We have presented 19 peering maneuvers that the Peering Coordinator Community have effectively used to obtain peering.

1) The **Direct Approach** uses peering@<ispdomain>.net , phone calls, face to face meetings, or some such direct interaction to establish peering.
2) The **Transit with Peering Migration** tactic leverages an internal advocate to buy transit with a contractual migration to peering at a later time.
3) The **End Run Tactic** minimizes the need for transit by enticing a direct relationship with the target ISP's largest traffic volume customers.
4) In Europe the **Dual Transit/Peering** separates the peering traffic from the transit traffic using separate interface cards and/or routers.
5) **Purchasing Transit Only from Large Tier 2 ISPs** is an approach to reduce the risk of being a customer of a potential peer on the road to Tier 1 status.
6) **Paid Peering** as a maneuver is positioned by some as a stepping stone to peering for those who don't immediately meet the peering prerequisites.
7) In the **Partial Transit** tactic, the routes learned at an exchange point are exchanged with the peer for a price slightly higher than transport costs.
8) The **Chicken** tactic involves de-peering in order to make the other peer adjust the peering relationship.
9) In the **Traffic Manipulation** tactic, ISPs or content players force traffic along the network path that makes peering appear more cost effective.
10) The **Bluff** maneuver is simply overstating future traffic volumes or performance issues to make peering appear more attractive.
11) The **Wide Scale Open Peering Policy** as a tactic signals to the Peering Coordinator Community the willingness to peer and therefore increases the likelihood of being contacted for peering by other ISPs.
12) The **Massive Colo Build tactic** seeks to meet the collocation prerequisites of as many ISPs as possible by building POPs into as many exchange points as possible.
13) The **Aggressive Traffic Buildup** tactic increases the traffic volume by large scale market and therefore traffic capture to make peering more attractive.
14) **Friendship-based Peering** leverages contacts in the industry to speed along and obtain peering where the process may not be in place for a peering.
15) The **Spam Peering Requests** tactic is a specific case of the **Wide Scale Open Peering** tactic using the exchange point contact lists to initiate peering.
16) **Purchasing Legacy Peering** provides an immediate set of peering partners.
17) The **Bait and Switch** tactic leverages a large corporate identity to obtain peering even though ultimately only a small subset or unrelated set of routes are actually announced.
18) The **False Peering Outage** tactic involves deceiving an ill-equipped NOC into believing a non-existing peering session is down.
19) The **Leverage Broader Business Arrangement** takes advantage of other aspects of the relationship between two companies to obtain peering in exchange for something else.

Acknowledgements

This paper is based upon many conversations with many folks during the Internet Operations Research on the previous white papers. Thanks to the following for their review, insights, and comments on this paper: Joe Klein (Adelphia), Ren Nowlin (SBC Internet), Mitchell Rose (Digital Island/Cable & Wireless), Peter Cohen (Telia), Stephen Stuart (MFN), Jeffrey Papen (Yahoo!), John Harkin (ATG), Ingrid Erkman (ICG), Jeb Linton (EarthLink), Paul Nguyen (Google), Paul Vixie (PAIX), Peter Juffernholz (TeleGlobe), Michael Winslow (Williams), Blake Williams (Williams), Scott J. Ellentuch (TTSG Internet Services), Chris Cousins (Carrier1), Michel Py, William F. Maton, Raven Alder (Intermedia), Kevin Epperson (Level 3/University of Colorado), Geoff Huston (Telstra), Joe St Sauver, Eric Aupperle (formerly President of Merit), James Rice (BBC Internet Services), Mike Hughes (LINX), Josh Horn (Terramark NOTA), Andrew Partan, Eric Anderson (BT Ignite), (and several folks who asked not to be recognized for contributions).

About the Author

<wbn@equinix.com>

Mr. Norton's title is Co-Founder and Chief Technical Liaison for Equinix. In his current role, Mr. Norton focuses on research on large-scale interconnection and peering research, and in particular scaling Internet operations using optical networking. He has published and presented his research white papers ("Interconnections Strategies for ISPs", "Internet Service Providers and Peering", "A Business Case for Peering") in a variety of international operations and research forums.

From October 1987 to September 1998, Mr. Norton served in a variety of staff and managerial roles at Merit Network, Inc., including directing national and international network research and operations activities, and chairing the North American Network Operators Group (NANOG) Internet industry forum. Mr. Norton received a B.A. in computer Science and an M.B.A. from the Michigan Business School, and has been an active member of the Internet Engineering Task Force for the past 15 years.

<wbn@equinix.com>

Appendix A – Open Peering Example

Organization	IP address	AS#	Email contact
Vixie Enterprises	198.32.176.3	3557	?
AboveNet	198.32.176.11	6461	noc@above.net
DSL.net Santa Cruz	198.32.176.13	4436	peering@dsl.net
Exodus	198.32.176.15	3967	peering@exodus.net
Hurricane Electric	198.32.176.20	6939	mleber@he.net
VIA Net.Works	198.32.176.22	5669	peering@vianetworks.com
ValuServe	198.32.176.28	6123	?
Lightning Internet	198.32.176.34	6427	peering@lightning.net
Critical Path	198.32.176.37	10627	noc@cp.net
WebTV	198.32.176.39	6469	soc@corp.webtv.net
XMission	198.32.176.42	6315	peering@xmission.com
DACOM Corporation	198.32.176.43	3786	peering@bora.net
Hostcentric	198.32.176.45	11388	peering@hostcentric.com
PFM Communications	198.32.176.48	4513	?
SingTel	198.32.176.50	7473	peering@ix.singtel.com
Zocalo	198.32.176.53	715	peering@zocalo.net
KDDNet	198.32.176.65	2516	peering@kddnet.ad.jp
WinterLAN	198.32.176.73	5081	noc@winterlink.net
Hanaro Telecom	198.32.176.75	9318	peering@hanaro.com
Hotmail	198.32.176.77	12076	dmcgilli@microsoft.com
Via.Net	198.32.176.80	7091	noc@via-net-works.com
Nokia	198.32.176.84	14277	nokiaisp@iprg.nokia.com
Open Data Network	198.32.176.86	4725	as-admin@gw.odn.ad.jp
Digital Island	198.32.176.99	6553	mrose@digisle.net
StarNet	198.32.176.100	6316	peering@starnetusa.net
Sunrise Communications	198.32.176.110	6730	helpdesk@sunrise.ch
Open Data Network	198.32.176.115	4725	as-admin@gw.odn.ad.jp
Advanced Telcom Group	198.32.176.116	6971	peering@atgi.net
DirecTV Broadband	198.32.176.119	12050	peering@telocity.net
Nominum	198.32.176.120	17204	peering@nominum.com
Thrunet	198.32.176.122	9277	noc@eng.thrunet.com
RCN	198.32.176.126	6079	peering@rcn.com
Akamai	198.32.176.127	12222	peering@akamai.com
Cogent Communications	198.32.176.131	16631	peering@cogentco.com
One Call Communications	198.32.176.133	6402	rirving@onecall.net
Yahoo! Inc.	198.32.176.135	10310	peering@yahoo-inc.com
SITA Equant	198.32.176.140	2647	Juan.Vadillo@sita.int
Primus Telecom	198.32.176.141	11867	peering@primustel.com
BBC	198.32.176.151	9156	Simon.Lockhart@bbc.co.uk
Compaq	198.32.176.241	33	noc@compaq.net
Compaq	198.32.176.242	33	noc@compaq.net
Internet Mainstreet	198.32.176.249	3856	

The above list was posted on the NANOG list to highlight those known to have open peering policies, implemented at one of the U.S. based exchanges..

Appendix B – Graphical Representation of ISP Peering

In order to present Peering and Transit relationships and the "Plays" that are invoked I needed to create a graphical representation.