B2B Service Provider Interoperability

The Trade-offs Involved with Daisy Chaining

A GXS Thought Leadership White Paper
What is Daisy Chaining?

Daisy chaining is a term used to describe an architectural methodology that B2B integration providers use to facilitate interoperability with one another. There are two basic architectures—peer-to-peer and daisy chaining.

In a peer-to-peer architecture, each B2B service provider is directly connected to the others and there are no intermediaries handling the transmission between any two end points. In a daisy-chain architecture, B2B service providers are strung out in a chain between the end clients. Each B2B service provider is responsible for the traffic both upstream and downstream for not only themselves, but for other providers that have data passing through their infrastructure.

Why Do Some B2B Service Providers Seek to Utilize Daisy Chaining?

Daisy chaining is a powerful concept. As new B2B service providers join the chain they get immediate—though only indirect—access to anyone else on the chain. For certain B2B startups this may be beneficial and their preferred architecture, as one connection gives them access to the entire community. It is also less expensive than a peer-to-peer architecture as the B2B service provider only needs to manage one or two links.

Why Do Some B2B Service Providers Seek to Avoid Daisy Chaining?

Daisy chaining interferes with a B2B service provider’s ability to fully define and control a superior client experience. Service experience can be defined in multiple ways. Let’s explore what this means:

Operational Controls: In a peer-to-peer architecture each party signs a contractual agreement with the other as to how the service will work, including mutual obligations in regard to support, operational reliability and service delivery. Both parties are contractually obligated to support one another to maintain traffic flow between them. In a daisy-chain
environment there is no contractual obligation or commitment between the B2B service providers on the chain, despite the fact that they are handling each other’s traffic. Every B2B service provider becomes exposed to the operational risks associated with the weakest link in the chain.

**Security and Privacy Controls:** B2B documents transmitted via B2B service providers are often encrypted at the session level but not at the file level. As result, each B2B service provider that takes possession of the data is able to review the content of the documents. In a daisy-chain environment, a B2B service provider cannot be assured that another B2B service provider down the chain is not allowing unauthorized access to the data. Consequently sensitive information, such as pricing, is at risk of being released to third parties or the public. No provider in the chain can ensure that this is not happening, given it is not party to any agreement beyond its direct-connect relationships.

In today’s business environment, B2B documents routinely contain sensitive information, such as bank statements, routing numbers, pricing information, customer lists, etc. B2B service providers that endorse daisy-chain architecture would arguably be hard-pressed to explain to risk managers and security consultants how data is protected.

**Latency:** Many B2B transactions have become more time sensitive. In a peer-to-peer architecture, data flowing from client A to client B is more direct and latency can be controlled. Contractual obligations between the parties can typically resolve any special handling that is necessary to ensure low latency.

In a daisy-chain environment, there are no contractual obligations that bind all of the B2B service providers in the chain. As a result, each provider adds to the latency and there are no controls or documents that govern latency. It is possible that client A and client B are both in the same country and physically only 30 miles away, yet they have selected different B2B services providers that use the daisy-chain architecture. Between these clients may sit yet another B2B service provider in a different country and time zone. This provider may elect to perform system maintenance during its non-business hours—resulting in the flow of in-transit data grinding to a halt—creating a major impact on the clients’ business.

**End-to-End Visibility:** Many clients want to track and trace their B2B documents in order to know where they are at any given time. Today, that is not possible in a daisy-chain environment. Once a document is handed off to another B2B service provider, both visibility and the status of the document is lost. However in a peer-to-peer setting most of the document flow is handled via X12.58—an industry standard used for interoperability—to provide a confirmation code for each exchange that occurs between the two B2B service providers. This confirmation code can be used to follow up with the other provider in the event of an issue or a question about the status of a document.

In a daisy-chain environment there is no exchange of track and trace information beyond the adjacent provider. If a document is being sent by provider 1 to a client on provider 4, there is no end-to-end confirmation or tracking code provided to provider 1. At best, B2B service provider 1 might get a confirmation code from B2B service provider 2, but
gets none from B2B service providers 3 and 4. In essence, being able to determine which provider has the data at any given time, cannot be confirmed.

**Troubleshooting/Root Cause Analysis:** Despite the best intentions of B2B service provider's, data can and does occasionally get lost due to operational issues. This can occur in both peer-to-peer and daisy-chain architectures. The ability to recover the data without client impact is more likely in a peer-to-peer environment. In the event data is lost, directly connected providers are contractually obligated to support each other to recover missing data; and often times they have technical solutions in place, such as X12.58 mail bagging, to support that process.

In a daisy-chain environment, no such obligation exists, given that the providers up and down the chain are not contractually bound to each other. In addition, root cause analysis requires coordination of all the parties involved. GXS’s experience with troubleshooting issues in a daisy-chain environment has been that there is little cooperation between providers and calls are generally unproductive.

The ability to diagnose a problem and perform root cause analysis in a daisy-chain environment is only as good as the investment in tools, operational processes and logs of the weakest provider in the chain. A provider can invest heavily on infrastructure, debugging tools and data logging. However, if one provider in the daisy chain elects not to invest, that becomes the “service standard” the chain is capable of supporting. GXS has been denied root cause analysis because B2B service providers in the daisy chain did not keep sufficient logging information.

**Brand Control:** In a peer-to-peer architecture, it is easy to address questions from clients because of the B2B service providers’ interoperability. A peer-to-peer approach requires each provider to sign contractual agreements with each other, making it easy to log and track documents.

In a daisy-chain environment, if a client asks B2B service provider 1 whether they can route data to a client on B2B service provider 4, the question would be difficult to answer. There is no centralized repository that reveals who the B2B service providers are that are connected to the daisy chain. In addition, there is no obligation on behalf of any B2B service provider to notify the others when additional B2B service providers come on- or off-line. As a result, B2B service provider 1 and B2B service provider 2 have no visibility as to whether clients on B2B service provider 4 are now able to send and receive documents between them. Only in a peer-to-peer architecture can brand control be proactively managed and maintained. Many B2B service providers want to choose with whom they interoperate. This is often important to B2B service providers that have a strong brand. They may want to prevent being associated with B2B service providers that have a reputation for poor client service, or when the association may be politically, morally or lawfully problematic.

In the daisy-chain architecture the ability to control a brand is lost since the ability to approve or disapprove interoperability is made by others.
Export Controls and Compliance with Local Law: Similar to the issues described under brand control, exposures exist in the ability to comply with trade restrictions. If decisions about interoperability are decentralized and cannot be controlled, legal exposures exist for B2B service providers.

Many countries have export controls that restrict foreign trade. As an example, the United States may have an embargo on trade with certain nations, but other countries may have no such restriction. In a daisy-chain setting there would not be a way for US-based B2B service providers to ensure that they are not a party to facilitating traffic flow with an embargoed country through a non-US B2B service provider as there is nothing restricting interconnect traffic in a daisy-chain setting. The US-based B2B service provider would most likely not have visibility into the downstream B2B service providers that are already connected and their activities.

In a peer-to-peer architecture, this would be easily avoided as the traffic between the non-US B2B service provider and the US B2B service provider would be governed by contracts that expressly prohibit traffic of the US provider to originate or terminate in an embargoed country.

Shouldn’t I Think of a B2B Service Provider as Having the Same Capabilities of an Internet Service Provider (ISP)?

No. The Open Systems Interconnection (OSI) reference model has been an essential element of computer network design since 1984. The OSI model is a technology standard maintained by the International Standards Organization (ISO). Although today’s technologies do not fully conform to the standard, it remains a useful introduction to the study of network architecture. There are seven layers to the model broken into two groups; the upper group which contains Application, Presentation and Session; and the lower group which contains Transport, Network, Data Link and Physical.

B2B service providers operate in the upper group and ISPs operate in the lower group. This means that the B2B service provider is responsible for routing, addressing, forwarding, storing and securing the B2B documents being transmitted; and these are not embedded capabilities provided by ISPs. Each B2B service provider has proprietary Intellectual Property (IP) to process these B2B documents and each does it differently. This means that if any given B2B service provider is down in the daisy chain—for any reason—all data stops flowing at the point of the non-operational B2B service provider. There is no embedded automated capability to reroute data, as exists in the ISP model. As a result, customer A’s transmission to customer B would never be seen in a daisy-chain environment if one B2B service provider in the chain is down.

Do End Users Care?

Admittedly, many corporations are not aware of the formalities or informalities that govern B2B service provider interoperability. They have entrusted their service to professionals
that they believe are making educated decisions that will protect their data. The users will never be aware of an issue unless there is excessive latency, lost data or a breach of sensitive information into the public domain. Questions regarding how this could happen will only arise once a problem occurs.

However, GXS and the other leading B2B service providers have demanding clients. These clients employ risk managers, data security auditors and risk security analysts, and require annual inspections of their providers’ infrastructures to inspect the processing of B2B documents. These clients are proactive in their attention to the security and integrity of their data, and they require their B2B service providers to provide a similar assurance.

**Summary**

Selecting whether to operate based on a peer-to-peer or a daisy-chain architecture is an individual business decision for each B2B service provider. GXS believes that the peer-to-peer architecture is better for its clients based on the service experience GXS chooses to provide. At GXS, we believe we provide the largest selection of peer-to-peer connections in the B2B service industry. Our interoperability now totals greater than 100 other B2B service providers.

Our peer-to-peer connectivity with other B2B service providers provides our customers and their trading partners with numerous connectivity options to conduct trade. Both trading partners do not need to be on the same network. However, we do seek to ensure that when we hand data off to another B2B service provider—on behalf of our client—we have done so in a prudent manner that will scale going forward.