Choosing a Transport

.NET Framework (current version)

This topic discusses criteria for choosing among the three main transports that are included in Windows Communication Foundation (WCF): HTTP, TCP, and named pipes. WCF also includes a message queuing (also known as MSMQ) transport, but this document does not cover message queuing.

The WCF programming model separates endpoint operations (as expressed in a service contract) from the transport mechanism that connects two endpoints. This gives you the flexibility to decide how to expose your services to the network.

In WCF, you specify how to transfer data across a network between endpoints by using a *binding*, which is made up of a sequence of *binding elements*. A transport is represented by a transport binding element, which is part of the binding. A binding includes optional protocol binding elements, such as security, a required message encoder binding element, and a required transport binding element. A transport sends or receives the serialized form of a message to or from another application.

If you must connect to an existing client or server, you may not have a choice about using a particular transport. However, WCF services can be made accessible through multiple endpoints, each with a different transport. When a single transport does not cover the intended audience for your service, consider exposing the service over multiple endpoints. Client applications can then use the endpoint that is best for them.

After you choose a transport, you must select a binding that uses it. You can choose a system-provided binding (see System-Provided Bindings), or you can build your own custom binding (see Custom Bindings). You can also create your own binding. For more information, see Creating User-Defined Bindings.

Advantages of Each Transport

This section describes the main reasons for choosing any one of the three main transports, including a detailed decision chart for choosing among them.

When to Use HTTP Transport

HTTP is a request/response protocol between clients and servers. The most common application consists of Web-browser clients that communicate with a Web server. The client sends a request to a server, which listens for client request messages. When the server receives a request, it returns a response, which contains the status of the request. If successful, optional data, such as a Web page, an error message, or other information is returned. For more information about the HTTP protocol, see HTTP - Hypertext Transfer Protocol.

The HTTP protocol is not connection-based—once the response is sent, no state is maintained. To handle multiple-page transactions, the application must persist any necessary state.

In WCF, the HTTP transport binding is optimized for interoperability with legacy non-WCF systems. If all communicating parties are using WCF, the TCP-based or named pipes-based bindings are faster. For more information, see NetTcpBinding and NetNamedPipeBinding.

When to Use the TCP Transport

TCP is a connection-based, stream-oriented delivery service with end-to-end error detection and correction. *Connection-*

based means that a communication session between hosts is established before exchanging data. A host is any device on a TCP/IP network identified by a logical IP address.

TCP provides reliable data delivery and ease of use. Specifically, TCP notifies the sender of packet delivery, guarantees that packets are delivered in the same order in which they are sent, retransmits lost packets, and ensures that data packets are not duplicated. Note that this reliable delivery applies between two TCP/IP nodes, and is not the same thing as *WS-ReliableMessaging*, which applies between endpoints, no matter how many intermediate nodes they may include.

The WCF TCP transport is optimized for the scenario where both ends of the communication are using WCF. This binding is the fastest WCF binding for scenarios that involve communicating between different machines. The message exchanges use the BinaryMessageEncodingBindingElement for optimized message transfer. TCP provides duplex communication and so can be used to implement duplex contracts, even if the client is behind network address translation (NAT).

When to Use the Named Pipe Transport

A named pipe is an object in the Windows operating system kernel, such as a section of shared memory that processes can use for communication. A named pipe has a name, and can be used for one-way or duplex communication between processes on a single machine.

When communication is required between different WCF applications on a single computer, and you want to prevent any communication from another machine, then use the named pipes transport. An additional restriction is that processes running from Windows Remote Desktop may be restricted to the same Windows Remote Desktop session unless they have elevated privileges.

> ⚠ **Warning**
>
> When using the named pipe transport with a weak wildcard URL reservation on multiple sites hosted in IIS, the following error may occur: An error occurred in the Activation Service 'NetPipeActivator' of the protocol 'net.pipe' while trying to listen for the site '2', thus the protocol is disabled for the site temporarily. See the exception message for more details. URL: WeakWildcard:net.pipe:/<machine name>/ Status: ConflictingRegistration Exception: Process Name: SMSvcHost Process ID: 1076\

Decision Points for Choosing a Transport

The following table describes the common decision points used to choose a transport. You should consider any additional attributes and transports that apply to your application. Identify the attributes that are important for your application, identify the transports that associate favorably with each of your attributes, and then select the transports that work best with your attribute set.

Attribute	Description	Favored transports
Diagnostics	Diagnostics allow you to automatically detect transport connectivity problems. All transports support the ability to send back fault information that describes connectivity. However, WCF does not include diagnostic tools for investigating network issues.	None

Hosting	All WCF endpoints must be hosted inside an application. IIS 6.0 and earlier support only hosting applications that use the HTTP transport. On Windows Vista, support is added for hosting all WCF transports, including TCP and named pipes. For more information, see Hosting in Internet Information Services and Hosting in Windows Process Activation Service.	HTTP
Inspection	Inspection is the ability to extract and process information from messages during transmission. The HTTP protocol separates routing and control information from data, making it easier to build tools that inspect and analyze messages. Transports that are easy to inspect may also require less processing power in network appliances. The level of security used impacts whether messages can be inspected.	HTTP
Latency	Latency is the minimum amount of time required to complete an exchange of messages. All network operations have more or less latency depending on the choice of transport. Using duplex or one-way communication with a transport whose native message exchange pattern is request-reply, such as HTTP, can cause additional latency due to the forced correlation of messages. In this situation, consider using a transport whose native message exchange pattern is duplex, such as TCP.	TCP, Named Pipe
Reach	The reach of a transport reflects how capable the transport is at connecting with other systems. The named pipe transport has very little reach; it can only connect to services running on the same machine. The TCP and HTTP transports both have excellent reach and can penetrate some NAT and firewall configurations. For more information, see Working with NATs and Firewalls.	HTTP, TCP
Security	Security is the ability to protect messages during transfer by supplying confidentiality, integrity, or authentication. Confidentiality protects a message from being examined, integrity protects a message from being modified, and authentication gives assurances about the sender or receiver of the message. WCF supports transfer security both at the message level and transport level. Message security composes with a transport if the transport supports a buffered transfer mode. Support for transport security varies depending on the chosen transport. The HTTP, TCP, and named pipe transports have reasonable parity in their support for transport security.	All
Throughput	Throughput measures the amount of data that can be transmitted and processed in a specified period of time. Like latency, the chosen transport can affect the throughput for service operations. Maximizing throughput for a transport requires minimizing both the overhead of transmitting content as well as minimizing the time spent waiting for message exchanges to complete. Both the TCP and named pipe transports add little overhead to the message body and support a native duplex shape that reduces the wait for message replies.	TCP, named pipe
Tooling	Tooling represents third-party application support for a protocol for development, diagnosis, hosting, and other activities. Developing tools and software to work with the HTTP protocol signifies a particularly large investment.	HTTP

See Also

BasicHttpBinding

;