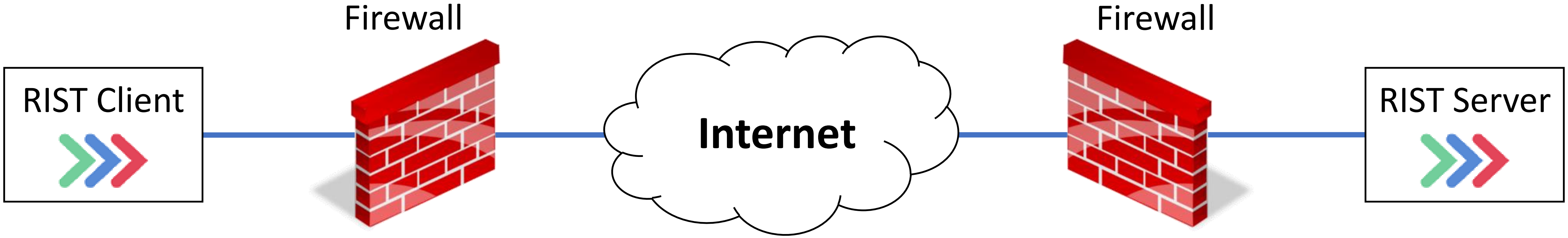
RIST Relay Overview

Ciro A. Noronha, Ph.D.
Cobalt Digital

IP SHOWCASE™

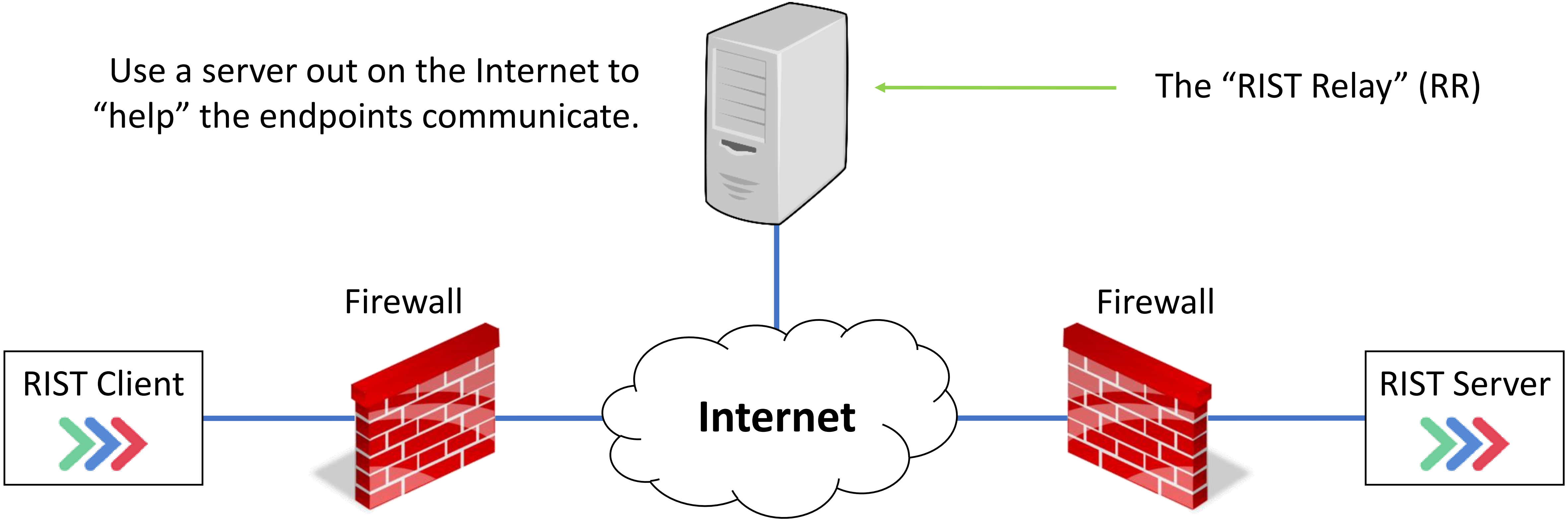
Audio Engineering Society   AIMS Alliance for IP Media Solutions   AMWA Networked Media. Working.   EBU   SMPTE   VSF VIDEO SERVICES FORUM

What is the Problem?



- RIST Client wants to connect to RIST Server
- Firewall at the client side is not a problem – it is an outgoing connection
- Firewall at the server side will not let the connection in
  - That’s what firewalls are for!
  - IT department will need to open and forward one more ports to allow this to happen
- Can we make this work without having to involve IT? Just like Skype?

Generic Solution



Use a server out on the Internet to “help” the endpoints communicate.

The “RIST Relay” (RR)

Why RIST?

- Users have explicitly requested mechanisms to simplify firewall crossing for RIST streams
    - RIST devices may be “guests” on some third-party network
- Advantages of a common Specification:
    - Mix-and-match of clients, servers and relay points
    - Vendors can create innovative solutions
    - Multiple business opportunities:
        - Provide the software
        - Provide a server
        - Provide a service

Why not STUN/TURN/ICE?

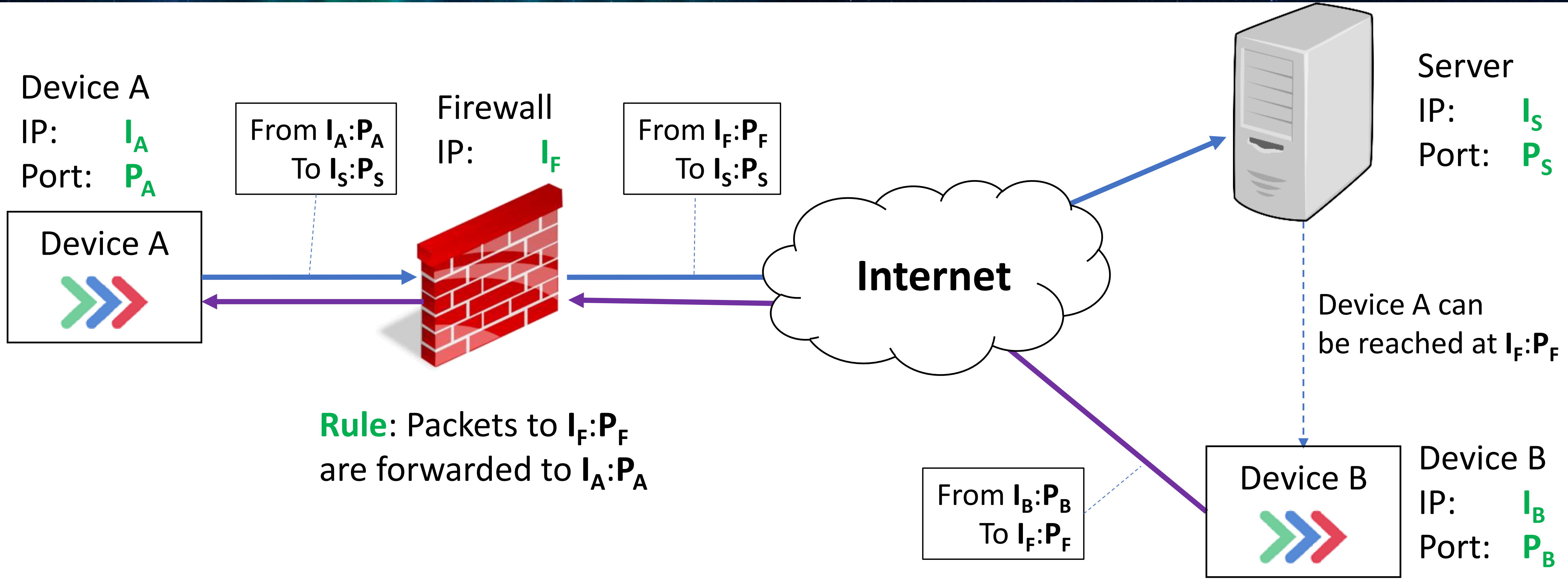
- There are RFCs that provide this functionality (ICE, aided by STUN/TURN) – what is wrong with that?
- These are not complete solutions:
  - STUN allows a node to figure out its public address
  - TURN is a relay server in case you can’t go directly
  - ICE is a means to negotiate STUN/TURN
  - You still need something like a SIP server so the nodes can discover each other
  - STUN/TURN have possible security issues
- For security, it is necessary to combine all the functions (STUN/TURN/ICE plus a server) into a single server.
- The RIST AG elected to re-use the RIST security and design a complete solution using Advanced Profile.

A Closer Look at Firewalls

As far as traffic management goes, there are two types of NAT firewalls:

- **Asymmetric Firewalls**:
  - Outgoing traffic creates a temporary rule that includes only the port
  - Any return traffic matching the port is admitted into the network
  - Most consumer-grade firewalls are asymmetric
  - Direct bypass is possible
- **Symmetric Firewalls**:
  - Outgoing traffic creates a temporary rule that includes both IP address and port
  - Only return traffic from that IP address is admitted into the network
  - Higher security
  - Direct bypass is not possible

Asymmetric Firewalls Allow Bypass



Device A
IP: I_A
Port: P_A

From I_A:P_A
To I_S:P_S

Firewall
IP: I_F

From I_F:P_F
To I_S:P_S

Server
IP: I_S
Port: P_S

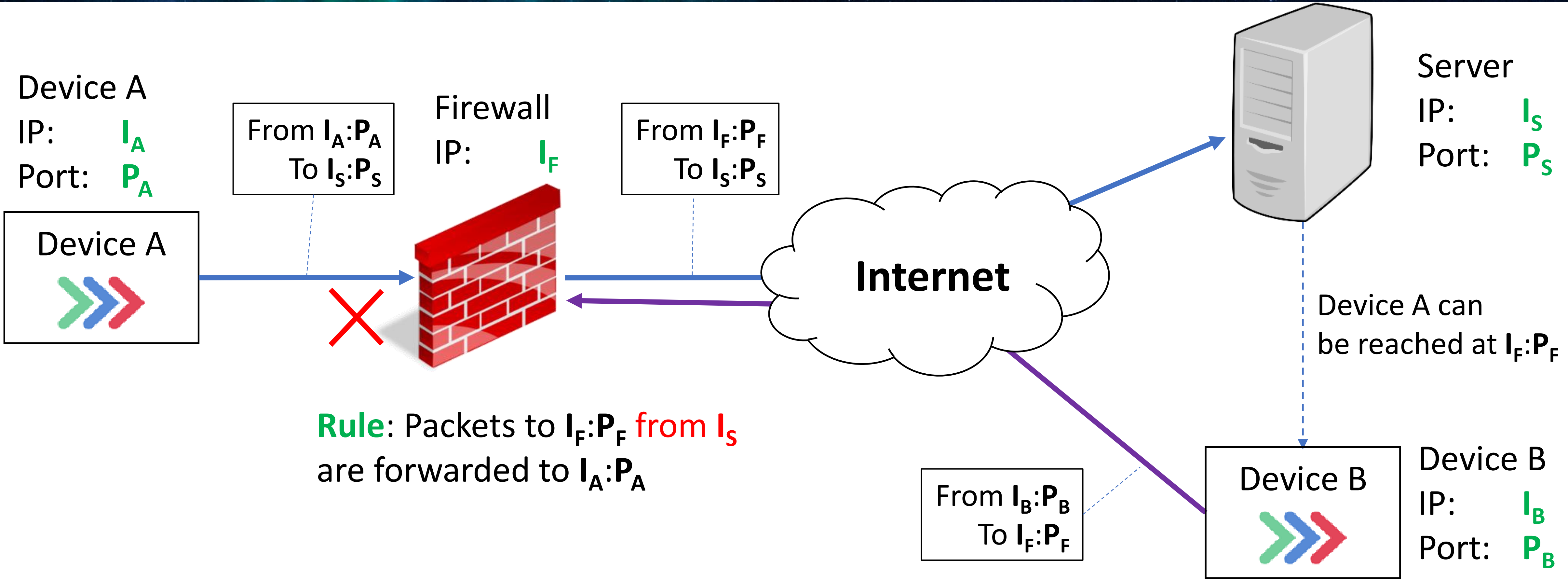
Device A can be reached at I_F:P_F

Rule: Packets to I_F:P_F are forwarded to I_A:P_A

From I_B:P_B
To I_F:P_F

Device B
IP: I_B
Port: P_B

Symmetric Firewalls Block Bypass



Device A
IP: I_A
Port: P_A

Device A

From $\mathbf{I_A}$:$\mathbf{P_A}$
To $\mathbf{I_S}$:$\mathbf{P_S}$

Firewall
IP: I_F

From $\mathbf{I_F}$:$\mathbf{P_F}$
To $\mathbf{I_S}$:$\mathbf{P_S}$

Internet

Server
IP: I_S
Port: P_S

Device A can
be reached at $\mathbf{I_F}$:$\mathbf{P_F}$

From $\mathbf{I_B}$:$\mathbf{P_B}$
To $\mathbf{I_F}$:$\mathbf{P_F}$

Device B

Device B
IP: I_B
Port: P_B

Rule: Packets to $\mathbf{I_F}$:$\mathbf{P_F}$ from $\mathbf{I_S}$
are forwarded to $\mathbf{I_A}$:$\mathbf{P_A}$

Firewall Implications

- Asymmetric Firewalls allow endpoints to connect directly
  - Very desirable from a bandwidth point of view
  - Server is only involved in connection establishment
  - Lower security in the firewall
- Symmetric Firewalls only allow endpoints to connect to a server
  - Server must be capable of **relaying** the content from endpoint to endpoint as direct communication is not possible
  - This is why we called it the "RIST Relay"

RIST Relay (RR) Requirements

- Endpoints must “login” and be authenticated by the RR since:
  - RR “works around” a firewall, so security is very important
  - Only registered and allowed endpoints should be permitted
  - Since endpoints can connect from anywhere, the RR must provide some sort of directory service to allow end-to-end connections
- RR must be able to facilitate direct bypass connections
  - There is no way to “know” if bypass is going to work until it is tried
- RR must be able to relay (forward) traffic between endpoints
- Endpoints should have some control of what happens

RIST Relay Security

- Endpoints must establish a **RIST Advanced Profile** connection with both encryption and authentication:
  - DTLS with certificate-based authentication
  - DTLS with TLS-SRP (username/password authentication)
  - PSK with EAP-SHA256-SRP-6 (username/password authentication)
  - Wireguard (in the publication queue as TR-06-4 Part 2)
- The authentication information identifies the endpoint to the RR
- Endpoints are identified by a human-readable name, pre-configured in the RR using out-of-band means

Quick Recap of RIST Advanced Profile

- RIST Advanced Profile is published as TR-06-3
- Advanced Profile basics:
  - It provides a tunnel encapsulated in RTP
  - It provides packet loss protection via ARQ and/or FEC to the tunnel
  - It supports multiple encryption and authentication options
  - It supports encapsulation of multiple protocols, including IPv4/v6, Ethernet, GRE, as well as a direct payload option
  - It includes a control channel, also encapsulated in RTP, with a custom packet format

RR Communication Protocol

- Communication with the RR is via Advanced Profile Control Messages
  - New set of messages defined for RR use
  - Messages not protected by ARQ, the protocol takes into account possibility of packet loss
- Messages are encrypted
- RR can say “no” to requests
- RIST keep-alive messages are used to keep the connection active

Control Index	Message	Mandatory
0x8030	Connection Initiation Message	Yes
0x8031	Request Denied Response	Yes
0x8032	Directory List Response	RR only
0x8033	Connection Request Response	Yes
0x8034	Connection Incoming Message	Yes
0x8035-0x803F	Reserved for RR-to-Endpoint Control Messages	
0x8040	Connection Initiation Response	Yes
0x8041	Connection Incoming Response	Yes
0x8042-0x804F	Reserved for Endpoint-to-RR Control Messages	

General Operation

- At connection, the endpoint receives one of the following:
  - “RR is ready”
  - “RR is busy, go away”
  - “Redirect to some other RR” (specified by IP address or hostname)
- After an endpoint successfully connects to the RR, it indicates:
  - “I wish to connect to some other endpoint”
  - “I am ready to accept connections”
  - “Give me the directory list of connected endpoints”
  - “I am not yet ready to do anything”

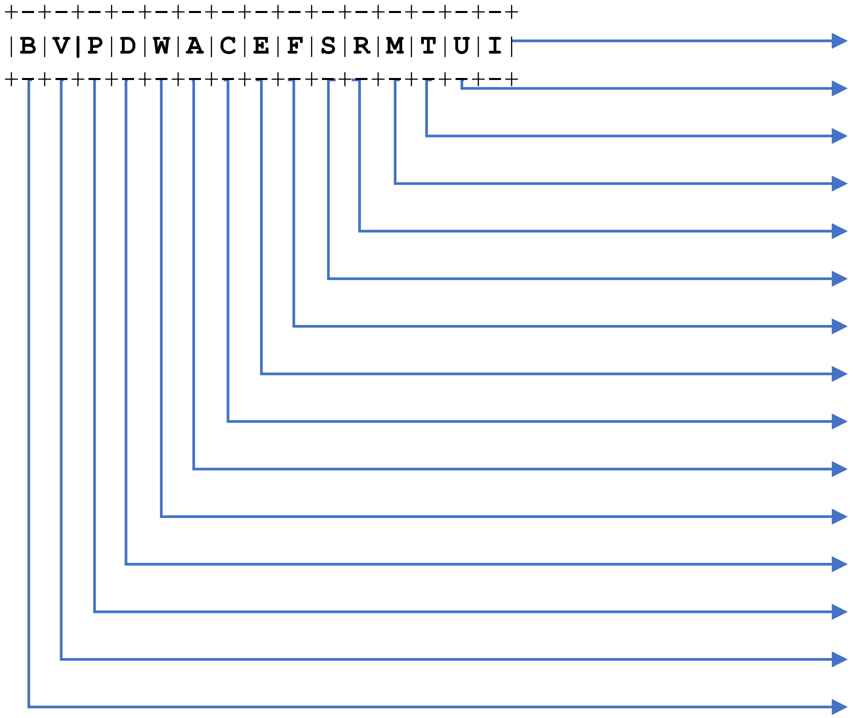
RR Can Say “No” (Request Denied)

- The RR can say “no” to any request from the endpoint using the Request Denied message
- The Request Denied message includes information to identify the request, and a reason code
  - Unspecified reason
  - Unauthorized
  - Not Found (endpoint exists but is not currently connected)
  - Does Not Exist (requested endpoint does not exist)
  - RR Out of Resources
  - Connection Refused by the Remote Endpoint
  - Invalid Request
  - Incompatible Protocol
  - Invalid Requester IP Address

Endpoint Protocol Support

- Advanced Profile has multiple inner protocol options
- Endpoint must declare which options it supports
- Endpoint must indicate whether it is willing to accept bypass
- RR can relay data packets across different encryption modes, but the actual data is opaque to the RR
- The support information is part of the Connection Initiation Response from the endpoint
- The support information is returned in the directory

Protocol Support Flags



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|B|V|P|D|W|A|C|E|F|S|R|M|T|U|I|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Media-ST2022-6 Encapsulation support

Media-ST2110 Encapsulation support

Media-TS Encapsulation support

Main Profile Encapsulation support

Ethernet Encapsulation support

IPv6 Encapsulation support

IPv4 Encapsulation support

ST 2022-5 FEC support

ST 2022-1 FEC support

ARQ support

Wireguard support

DTLS support

PSK support

IPv6 bypass support

IPv4 bypass support

This information is sent by the endpoint to the RR at connection initiation and returned as part of a directory query

The “Blob”

- When an endpoint registers with the RR, it may optionally include an ephemeral “blob” of data
  - The “blob” only exists while the endpoint is connected
- If another endpoint asks to connect to this endpoint, the RR will pass along the “blob” to the requesting endpoint
- Defined “blob” types:
  - Endpoint certificate in PEM format
  - CA certificate in PEM format
  - Concatenation of CA and endpoint certificates in PEM format
- Vendor-proprietary blobs are supported but discouraged

Multipoint Operation

- The RR supports multipoint-to-multipoint operation by using groups
- A group is identified by a name just like an endpoint
  - Groups are created manually through out-of-band means
  - Directory listings have a bit to indicate whether a name is an individual endpoint or a group
- The RR is responsible for replicating received data to all other group members

Multipoint Implementation Options

- Full Proxy
  - RR terminates Advanced Profile connections with all endpoints, including packet loss recovery
  - Maximum ARQ bandwidth efficiency and lowest latency
  - RR can provide format conversion if desired
- Transparent
  - RR simply forwards Advanced Profile payloads from sender to all receivers
  - Packet loss recovery is end-to-end
  - Bandwidth-inefficient and worst-case latency
- Partial proxy cases are also possible

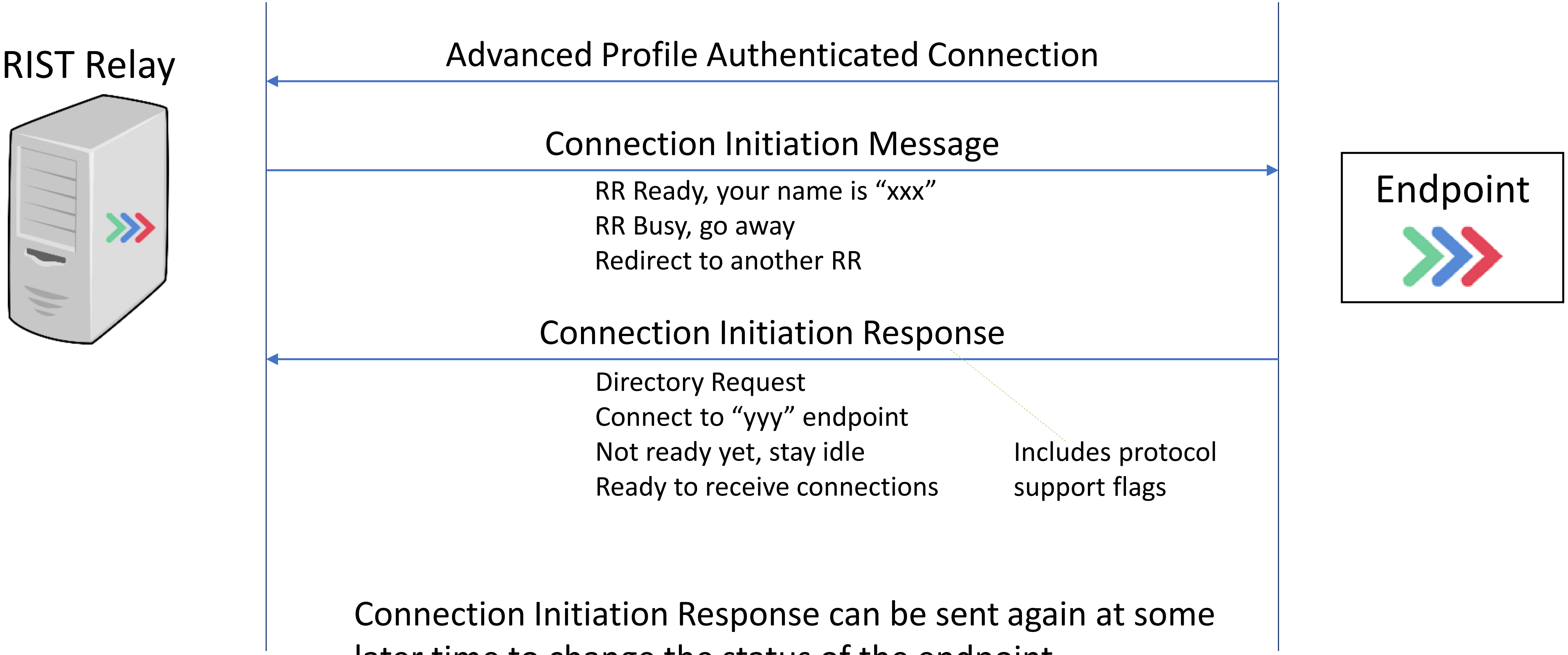
Directory Query

- Endpoints can ask the RR for a directory of connected endpoints
- Responses include:
  - Endpoint Name
  - Endpoint Type (individual or group)
  - Endpoint Protocol Support Flags
- Directory access control and filtering are up to the RR and will not be part of the Specification

Concurrent Connections

- An endpoint is allowed to have multiple “idle” or “ready to receive” connections to the RR
  - Used for redundancy
- If the RR receives a connection request to this endpoint, it will choose one of the “ready to receive” connections at its discretion
  - Protocol Support Flags may be used to inform this choice
- Each endpoint is listed only once in the directory

Protocol Exchange: Connecting to the RR



RIST Relay

Endpoint

Advanced Profile Authenticated Connection

Connection Initiation Message

RR Ready, your name is “xxx”
RR Busy, go away
Redirect to another RR

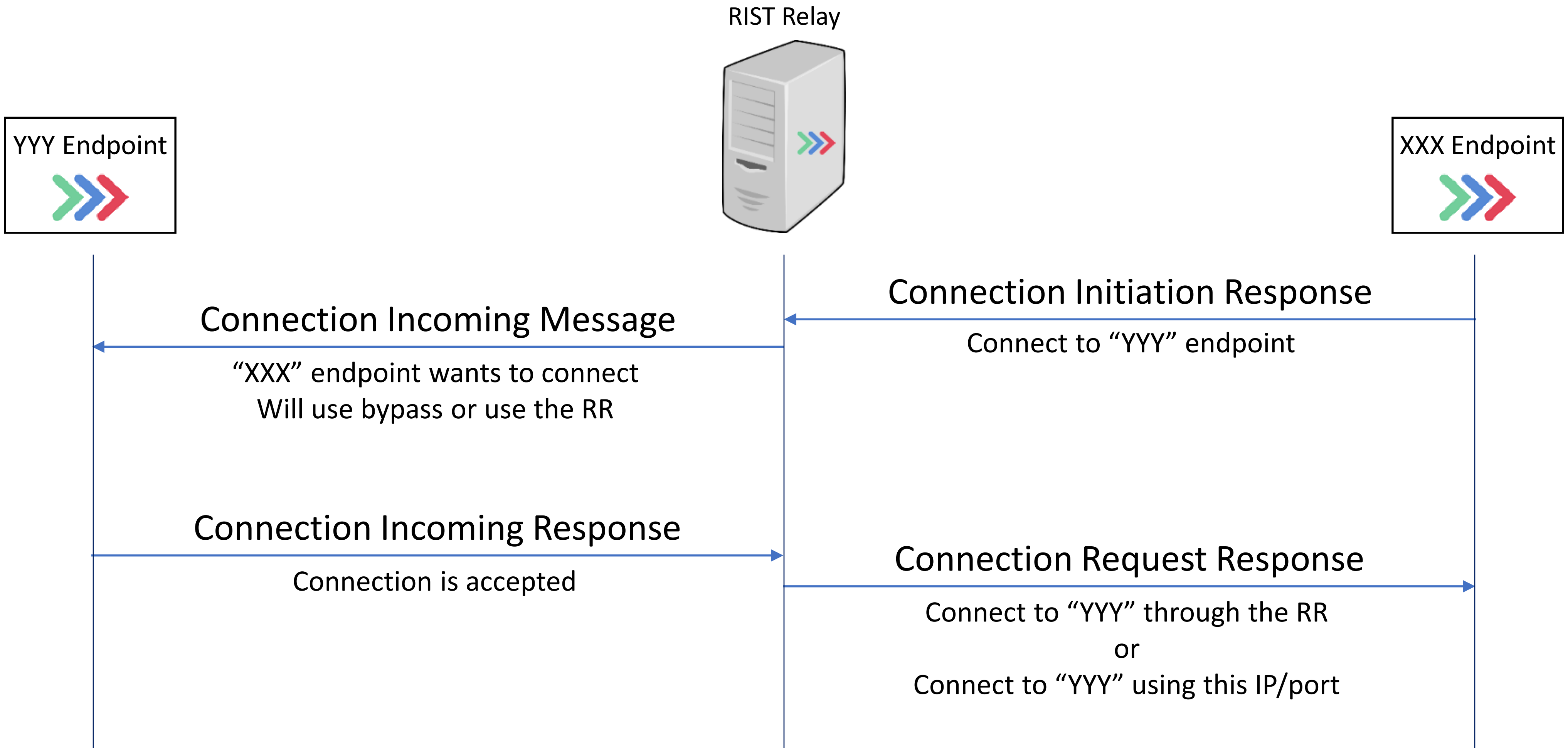
Connection Initiation Response

Directory Request
Connect to “yyy” endpoint
Not ready yet, stay idle
Ready to receive connections

Includes protocol support flags

Connection Initiation Response can be sent again at some later time to change the status of the endpoint

Protocol Exchange: Connecting to Endpoint



Connection Initiation Response

Connect to “YYY” endpoint

Connection Incoming Message

“XXX” endpoint wants to connect
Will use bypass or use the RR

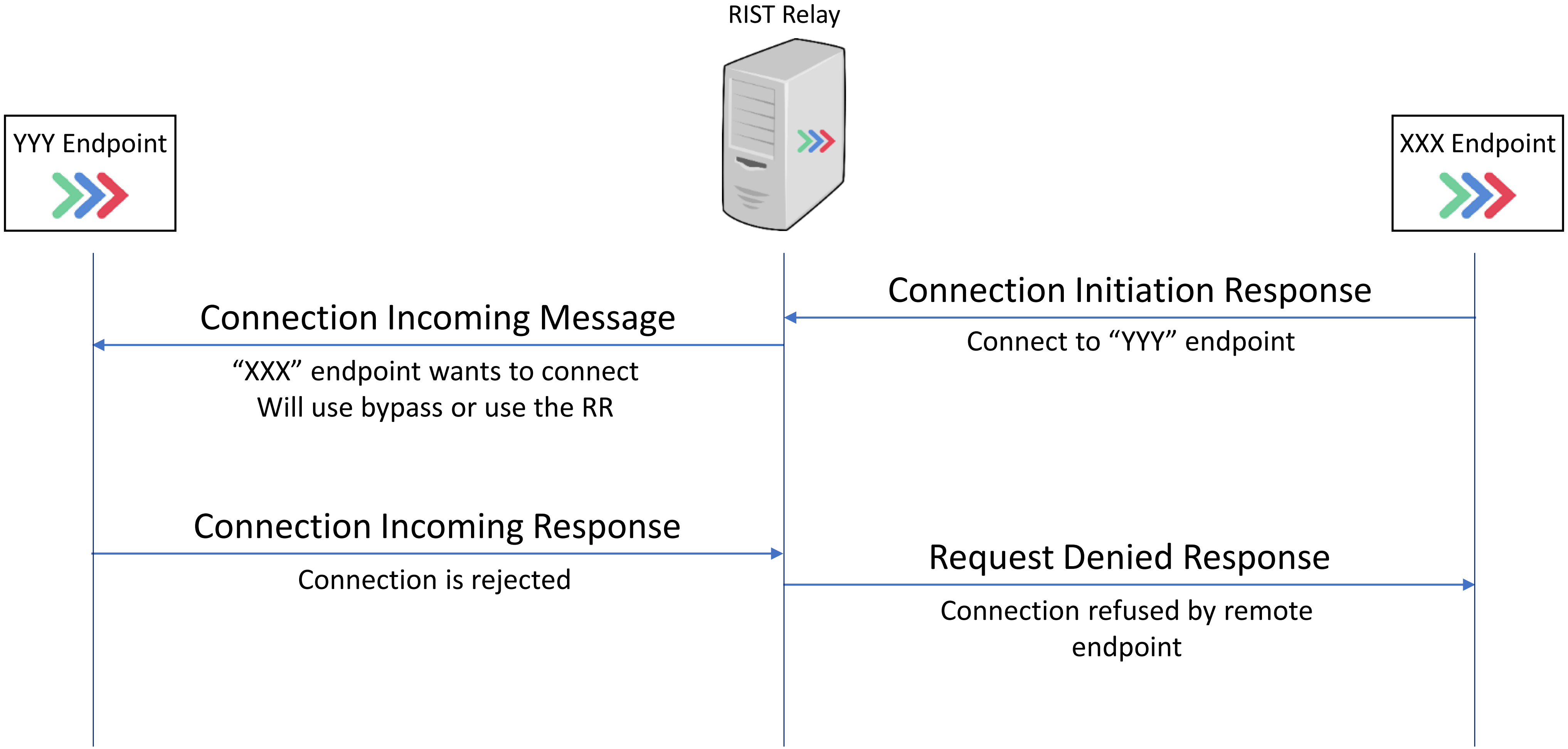
Connection Incoming Response

Connection is accepted

Connection Request Response

Connect to “YYY” through the RR
or
Connect to “YYY” using this IP/port

Protocol Exchange: Connecting to Endpoint



RIST Relay

YYY Endpoint

XXX Endpoint

Connection Initiation Response

Connect to “YYY” endpoint

Connection Incoming Message

“XXX” endpoint wants to connect
Will use bypass or use the RR

Connection Incoming Response

Connection is rejected

Request Denied Response

Connection refused by remote endpoint

Conclusions

- The RIST Relay RR will simplify support for establishing RIST connections for endpoints behind firewalls
- By using a common Specification, one can mix-and-match RR and endpoint vendors
- Specification will only include the minimum for interoperability, allowing vendors to innovate
- This is still work in progress and no implementations exist yet

Any Questions?

IP SHOWCASE™