Deploying Secure RSTP

Mick Seaman

This note is a first cut at specifying a set of security policies for use with RSTP/MSTP in conjunction with MACsec. These policies are designed not only to support bridged networks where security has been fully deployed, but also to facilitate the incremental introduction of MACsec, allowing each stage in the deployment to be tested before tightening security.

Protocol Deployment

Network administrators rarely have the freedom to take entire networks of significant size out of service for an extended period to perform simultaneous upgrades of systems, and applying a complex set of upgrades without stage by stage testing and an easy rollback plan is foolhardy. The client policies that each protocol that runs over MACsec adopts need to reflect that reality as well as the desire to achieve as complete security as economically practical at this layer.

In deploying MACsec it is useful to recognize not only the challenges inherent in network deployment where different systems may need to be upgraded at different times, not least because of the availability of features from different vendors, but also the opportunities presented by the staged availability of capabilities within a single system. Hardware for full data rate integrity protection of all traffic on a LAN may be available somewhat later than the capability to protect the frames sent by certain configuration protocols, for example.

The policies and accompanying protocol mechanisms described in this note support the following migration stages. Fortunately MACsec, by design, can be deployed one LAN at a time throughout a network.

A staged plan

The following is an outline of a deployment plan, the policies used are described below[1].

1. Establish a baseline. Inventory the set of bridges, routers, and end stations attached to each LAN to be secured.
2. Deploy auto upgrading RSTP, with MACsec protected BPDUs, and null policies to as many of the bridges as possible.
3. Check the baseline. If all bridges attached to a LAN have been upgraded, then all BPDUs on that LAN should now be MACsec protected.
4. Evaluate the network role of any Bridges attached to the LAN that are not sending MACsec'd BPDUs. If these can be tolerated but screened by policies, turn on dual mode BPDU transmission on the other bridges and implement restrictedRole and other polices on the MACsec capable Bridges.
5. Upgrade each of the MACsec Bridges to be capable of providing MACsec protection of all data.
6. Check baseline. So far as possible verify that no MACsec incapable bridges that carry important network data remain attached to the LAN[2]. Verify this for all LANs in the group that a network operator might do a physical or logical plug swap on in a time of crisis.
7. Move attachment of the bridge's MAC Relay Entity from the SecY's Uncontrolled Port to the Controlled Port, and stop receiving BPDUs from the Uncontrolled Port. These two actions should be linked together for any given bridge port, but can occur at slightly different times for different Bridge Ports attached to the same LAN[3].

Stages 1, 2, and 3 guard against having to roll back further deployment, and provided useful information in the event of a later problem. Once stage 4 has been implemented the network is protected against attacks originating from the LAN against the RSTP configuration in the rest of the network. Once stage 7 is implemented the traffic on the LAN is independent of unauthorized systems.

The potential complexity is much reduced when LANs are point to point and are intended to provide communication between two stations[4] at most.

[1] What is really wanted is a flow chart. Time permitting.

[2] It is possible that a non-standard bridge with xSTP disabled has not been detected in stage 3.

[3] Service will be disrupted while some Bridge Ports have moved to full use of MACsec while others have yet to make the transition.

[4] A 'station' is anything directly attached to a LAN, e.g. a Bridge Port, and should not be confused with a 'system'. Obviously two bridge ports can relay traffic for many systems.

RSTP and MAC Relay Policies[5]

Secure RSTP implements policies that use the authorization provided by P802.1af and the associated integrity and origin guarantees provided by MACsec. RSTP policies are applied to received BPDUs and control whether or not:

1. The receiving port can be a Root Port.
2. Topology changes are accepted.

The MAC Relay can forward frames from either the Uncontrolled Port or the Controlled Port, or both. If frames are forwarded from the Controlled Port, then frames that begin with the MACsec Ethertype are not forwarded from the Uncontrolled Port.

If frames are forwarded from the Uncontrolled Port then BPDUs are received from the Uncontrolled Port, or at least RSTP is prepared to receive such BPDUs. Similarly if frames are forwarded from the Controlled Port then BPDUs are also received from that Port.

Different levels of authorization are naturally attached to BPDUs received from the Controlled and Uncontrolled Ports. Since, during stage 4 of deployment, MACsec protected BPDUs are used to establish spanning tree port states for Uncontrolled Port data, it is not possible to treat the two ports as separate Bridge Ports. Modifying RSTP to record a separate received priority vector for Controlled and Uncontrolled BPDUs appears unnecessarily complex, so it seems there will be times when the reception of an Uncontrolled BPDU can displace a priority vector received in a Controlled BPDU and cause the receiving port not to be a Root Port. The authorization level associated with each received priority vector is maintained along with the RSTP “infoIs” variable for the port to ensure that the policy control is applied correctly.

When the LAN is supporting a mix of MACsec capable and MACsec unaware bridges but it is desirable to use MACsec to protect communications amongst the former set, BPDUs need to be transmitted on both Controlled and Uncontrolled Ports. A Bridge Port receiving both effectively attributes a higher priority and subtly different identity to the Controlled BPDUs, thus ensuring that they, and their associated authorization level, are not immediately displaced by the Uncontrolled BPDU from the same transmitter.

[5] This note does not attempt to formally factor out those policies that are primarily associated with RSTP and those with the bridge’s relay. Where policies are to be applied together or not at all it is desirable that there be only one control, the other entity being provided the information using the LMI.