

Status update of quarantine security model (1)



- Updated I-D (from 59th IETF in Seoul)
 - draft-kondo-quarantine-overview-01.txt
 - Referenced problem statement documents
 - Revised quarantine model components
 - Revised quarantine inspection process
 - Revised security policy enforcement points
 - routing information setup
 - VLAN
 - addressing and network prefix configuration (DHCPv6, RA/RS)
 - Added security considerations
 - Working together with IPv6-Security Problem-Statement/Requirement people to meet/update their demands.

Status update of quarantine security model (2)



- Prototype implementation ongoing
 - Working item as WIDE project secure6-wg
 - Target: 2004/Q4 – 2005/Q1
 - Goal
 - Deploying network separation and segmentation as security policy configuration.
 - IPv6 prefix assignment for each security segment
 - Evaluate existing protocols and methods.
 - PANA / 802.1X
 - DHCPv6
 - TSP or DTCP
 - VLAN (802.1Q)
 - Submitting useful document and report.

IPv6 Network Separation

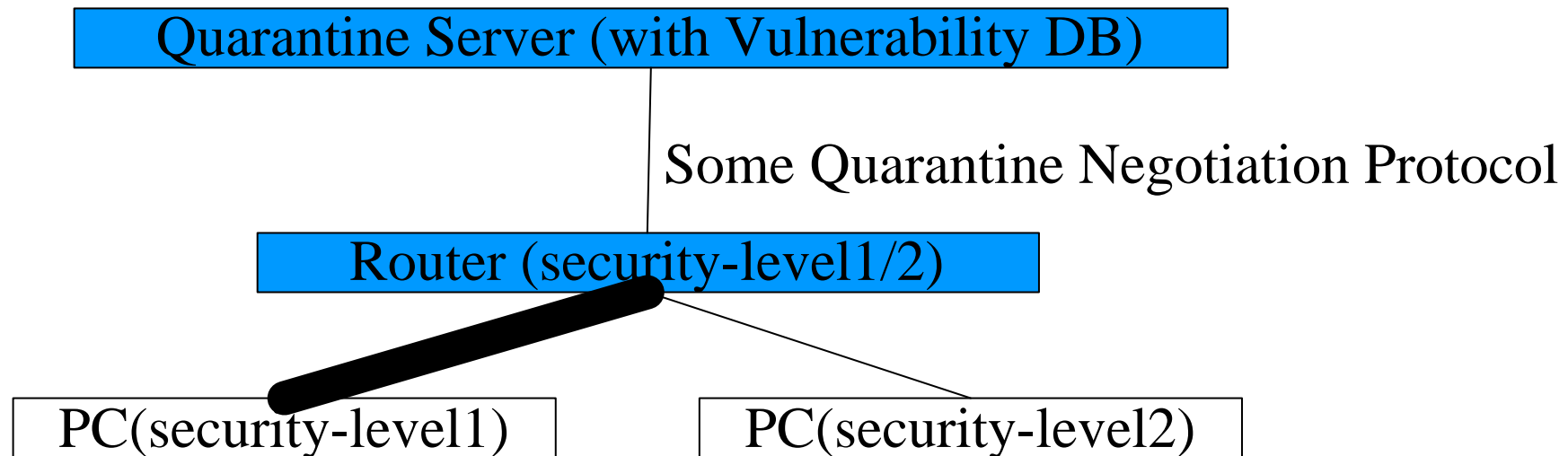


- Basic Concept of “Quarantine Model”
 - Separates the network connectivity of a node, based on its security level
- Key Point
 - How to measure “security level”
 - How to “separate network connectivity”

Network Separation based on RA



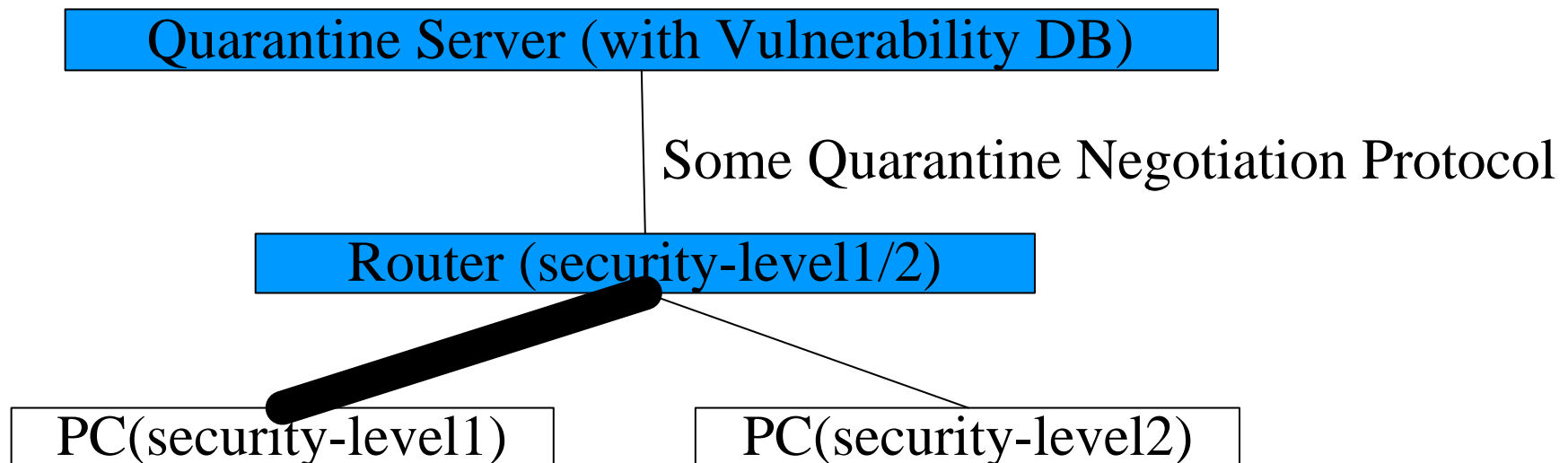
- Dispatches the upstream router connectivity using different prefixes via unicast RA
 - No ICMPv6-Redirect
 - OnLink-Flag=OFF for all prefixes
 - Filters every packet at Router based on prefix



Network Separation based on DHCPv6



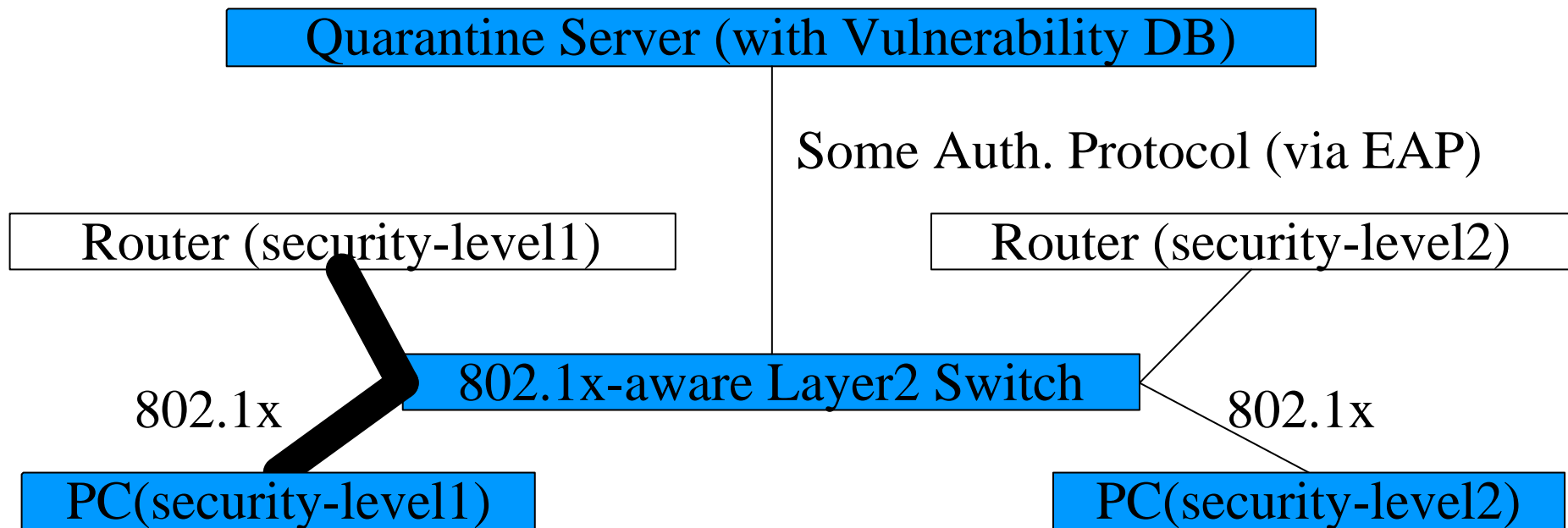
- Dispatches the upstream router connectivity using different prefixes through DHCPv6
 - No ICMPv6-Redirect
 - Filters every packet at Router based on prefix



Network Separation based on 802.1x



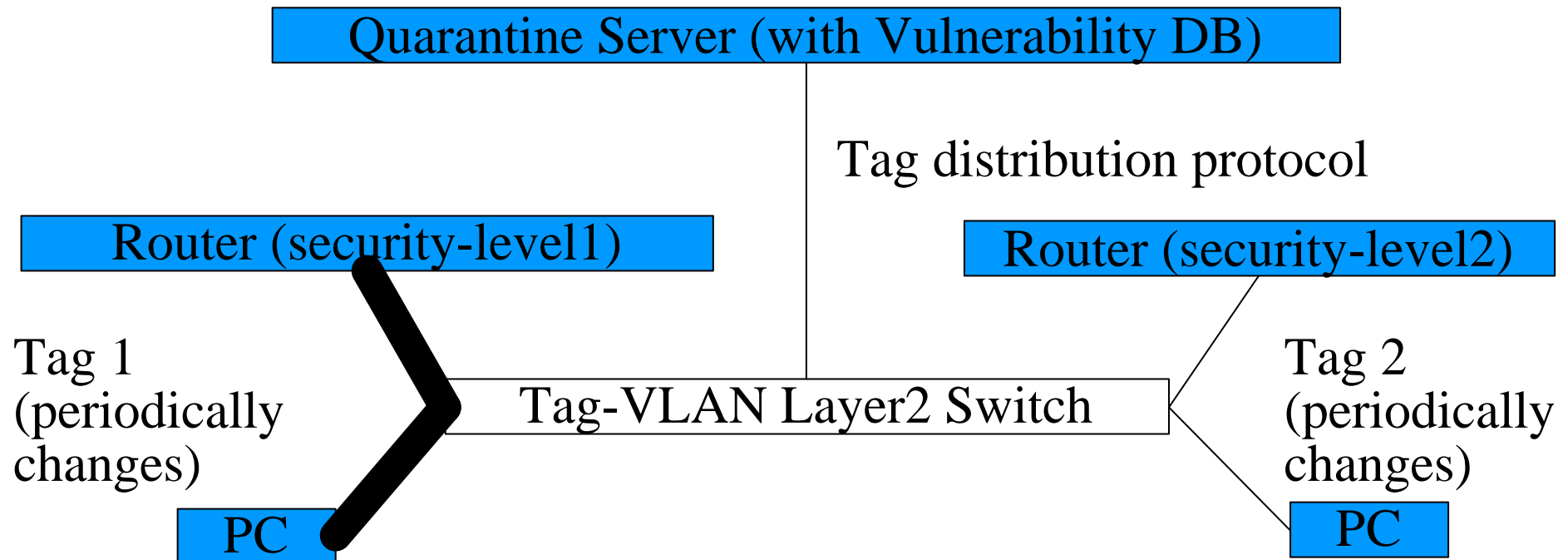
- Dispatches the upstream router connectivity using 802.1x



Network Separation based on 802.1q Tag distribution



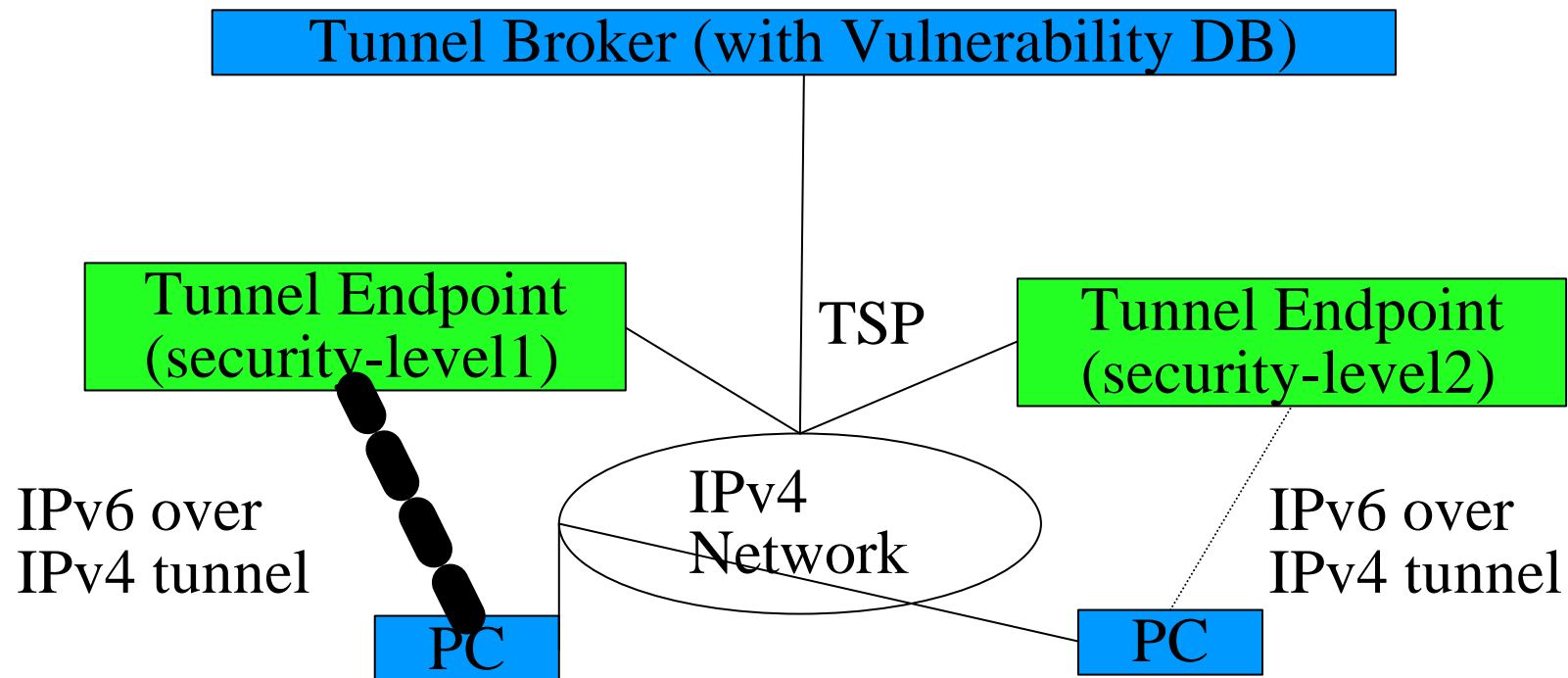
- Dispatches the upstream router connectivity using 802.1q Tag



Network Separation based on TSP



- Dispatches the upstream router connectivity using TSP



Comparison



	RA	DHCPv6	802.1x	Tag Distribution	TSP
IPv4 security	No change	No change	Enhanced	Enhanced	No change
Fake on PC	Easy	Easy	Difficult	Difficult	Difficult
Easy to change prefix?	No	Yes	No(RA) Yes(DHCPv6)	Yes	Yes(?)
Change in legacy protocol?	Yes	No	No	No	No
Just a legacy Protocol Extension is enough to implement it? (not necessary to create a separate new protocol?)	No	Yes	Yes	No	Yes
Easy to deploy?	No	Yes(?)	No	No	Yes

Next steps



- comments/inputs/proposals are appreciated
- ToDo
 - further analysis for specific network separation method
 - implementation/evaluation based on above analysis
- Partners are welcome!