Deploying APs over Low-Speed Links

BACKGROUND

Aruba's Mobile Edge architecture consists of thin access points wherever wireless coverage is needed and centralized Aruba mobility controllers for security, management and WLAN functions. The architecture has been designed with the utmost flexibility for different deployment models where Aruba mobility controllers and access points can be interconnected over any IP network (LAN or WAN) using Layer 3 communications. Today, a number of customers have deployed APs that connect to controllers located across low-speed (defined as less than 1Mbps capacity) or high-latency (defined as greater than 100ms) links. This document provides recommendations for deploying the Aruba Mobile Edge architecture across low-speed and high-latency links, discusses the potential problems involved in this type of deployment, and also discusses upcoming product enhancements to alleviate some potential problems.

LINK SPEED CONSTRAINTS FOR REMOTE NETWORKS

Aruba recommends that controllers and APs be connected over a link with a capacity of 1Mbps or greater, and requires a minimum link speed of 64 kilobits per second per tunnel-mode SSID. LANs, many metro area networks, and most broadband DSL or cable connections today provide link speeds greater than 1Mbps. For low-speed links such as ISDN, T1/E1, and many frame relay WAN connections, specific design guidelines and Aruba configuration are required to avoid connectivity problems.

To achieve high reliability and fast failover in the event of a network or controller outage, APs and controllers maintain "heartbeat" or "keepalive" packets between themselves. Failure to receive these heartbeat packets – described in detail below – can cause APs to "re-bootstrap", going through a process of tunnel re-establishment with the controller. During the bootstrap process, the AP will shut off all radios for approximately 20ms, and all clients will be required to re-associate.

Two types of heartbeat packets are sent: GRE tunnel keepalives and PAPI keepalives.

GRE Tunnel Keepalives

- Sent once each second
- Bi-directional: Sent from AP to controller and from controller to AP
- By default, AP will rebootstrap after missing 8 consecutive keepalive packets
  - Can be adjusted using "bootstrap-threshold" parameter
- By default, the controller will remove an AP's tunnel after 12 seconds of inactivity
  - Can be adjusted using "stm ap-inactivity-timeout" (ArubaOS 2.x)
  - In ArubaOS 3.0, this setting is equal to 1.5x the bootstrap-threshold
- Does not apply to bridge mode SSIDs (Remote AP)

PAPI Keepalives

- Sent once every minute, and retransmitted every five seconds when not acknowledged
- By default, APs will rebootstrap after communication with the controller is interrupted
  - In ArubaOS 2.5, the timeout will occur after 10 consecutive missed keepalives, approximately 50 seconds. In ArubaOS 3.1, this takes approximately four minutes.
  - Can be adjusted using "max-imalive-retries" parameter (ArubaOS 2.x) or "max-request-retries" (ArubaOS 3.x)
- Effectively applies only to bridge-mode SSIDs
  - For tunnel-mode SSIDs, GRE tunnel keepalive intervals will time out long before PAPI keepalive intervals

If a low-speed link is saturated, it is possible that AP heartbeat packets will be dropped, causing the AP to re-bootstrap. This is the primary cause of connectivity problems for APs connected across low-speed links.

An additional consideration for low-speed links is the throughput possible over the wireless LAN for tunnel-mode SSIDs. Tunnel-mode SSIDs transport all wireless traffic over GRE or IPSEC tunnels back to the mobility controller for processing. When used with low-speed links, tunnel-mode SSIDs are best suited for low-bandwidth applications such as barcode scanning, small database lookups, and telnet to avoid saturating the WAN link. As an alternative, APs can be deployed as Remote APs using the ArubaOS Remote AP module, and SSIDs can be configured as bridge-mode SSIDs. In a bridge-mode SSID, all wireless traffic is terminated locally at the AP and bridged onto the local Ethernet segment. If much of this traffic will remain local rather than crossing the WAN, saturation issues can be largely avoided. In addition, heartbeat timers for bridge-mode SSIDs can be set to be much more tolerant of packet loss.

There are no hard rules to categorize what will work and what will not. A number of Aruba customers have deployed APs across 64Kbps WAN links without difficulty, because packet loss is low and the throughput requirements are not high. Other customers with unpredictable traffic loads have experienced some problems due to AP heartbeat timeouts. Each customer will need to analyze realistic traffic patterns before deployment to minimize risk of link saturation.

LATENCY CONSTRAINTS FOR REMOTE NETWORKS

When deploying APs across high-latency links of 100ms or greater, special considerations are required due to the timing constraints of some client devices. Aruba APs locally process 802.11 probe-requests and probe-responses, but the 802.11 association process requires interaction with the mobility controller. Certain models of handheld computers and barcode scanners based on Windows PocketPC 4.2 are known to have very tight timing requirements that cause the association process to time out if an association response is not received within 102ms. Other devices and operating systems may be affected as well. Please check with your device vendor for the latest versions of firmware and drivers that are designed to be less sensitive to WAN latency.

Aruba recommends that customers test high-latency links to ensure that timing issues will not become a problem. For deployments where latency problems cannot be avoided, Aruba recommends that a mobility controller be installed closer to the APs.

RECOMMENDATIONS

When deploying APs across low-speed links, the following recommendations apply:

- Adjust the AP bootstrap-threshold if the network experiences packet loss. This will make the AP recover more slowly in the event of an actual failure, but it will be more tolerant to loss of heartbeat packets. The recommended setting is 30.

```
ap location 0.0.0 bootstrap-threshold 30                (ArubaOS 2.x)
ap system-profile default bootstrap-threshold 30        (ArubaOS 3.x)
```

- Reduce the number of tunnel-mode SSIDs if possible – each SSID creates a tunnel to the mobility controller with its own tunnel keepalive traffic.
- If much of the data traffic will remain local to the site, deploy Remote APs in bridging mode.
- If high-latency links (transoceanic or satellite) are used in the network, deploy a mobility controller geographically close to APs – for example, a mobility controller per continent.
- If high-latency is causing association issues with certain handheld devices or barcode scanners, inquire about recent firmware and driver updates that have been made available by device manufacturers to reduce the sensitivity to link latency.

PRODUCT ROADMAP

Aruba is planning a number of product enhancements to improve system performance when low-speed or high-latency links are used in the network. These enhancements are expected to be publicly available in June 2007.

- Tagging of AP management frames for external prioritization – Aruba APs and controllers will have the option to tag management frames, such as keepalive packets, using IP TOS. External networks will then be able to recognize these frames as higher-priority to minimize the chances that they will be dropped.
- AP-based processing of wireless association – Aruba APs already process probe requests and probe responses locally. With this enhancement, APs will also process association requests locally. This will allow for better client device interoperability even when APs are deployed across high-latency links.