Implementing VLANs with the Extreme Networks ReachNXT 100-8t using NetLogin

Introduction

The ReachNXT™ 100-8t is an 8-port 10/100 enterprise port extender with GigE uplinks that can be powered via Power over Ethernet (PoE). The ReachNXT 100-8t is controlled by the directly connected, upstream ExtremeXOS® switch. The ReachNXT 100-8t does not run ExtremeXOS; it essentially serves as an extension of an ExtremeXOS switch, providing additional access ports, aggregating network traffic from those ports, and sending it to the uplinked ExtremeXOS switch. Typical applications for the ReachNXT 100-8t include conference rooms, small departments and similar applications.

The ReachNXT 100-8t is dependent on an Extreme Networks® switch running ExtremeXOS for its functionality and is a visible network element in Extreme Networks EPICenter® network management software. The ReachNXT 100-8t does not directly support VLANs; all of its ports are untagged and are part of the same broadcast domain. When multiple clients are connected to the ReachNXT 100-8t enterprise port extender they are all on one network segment. However by taking advantage of features on the ExtremeXOS switch, traffic from these clients can be segregated to different VLANs by the ExtremeXOS switch. These ExtremeXOS features include NetLogin, MAC-based VLANs, Guest VLAN, multiple supplicant support and authentication failure VLAN.

Guest access can also be granted and this traffic segregated on a separate VLAN. In the case of a ReachNXT in a conference room, for example, if an employee connects to the ReachNXT and authenticates he is placed in VLAN A. If a guest, however, connects at the same time to the ReachNXT they are moved to VLAN B which allows access only to the public Internet.

This technical brief provides descriptions of the features that may be used in order to implement VLANs with the ReachNXT 100-8t along with deployment examples and caveats.

NetLogin MAC-Based VLANs and Multiple Supplicant Support

ExtremeXOS supports NetLogin MAC-based VLANs with multiple clients (supplicants) that individually authenticate on the same port. This feature makes it possible for two or more NetLogin-authenticated client stations to be connected to the same port and be assigned to different VLANs based on a VLAN RADIUS attribute. Authentication can be via 802.1x, MAC-based or via Web (Captive Portal). Client devices connected to the ReachNXT are all connected to the same ExtremeXOS switch port, however by using MAC-based VLANs these clients can be assigned to different VLANs.

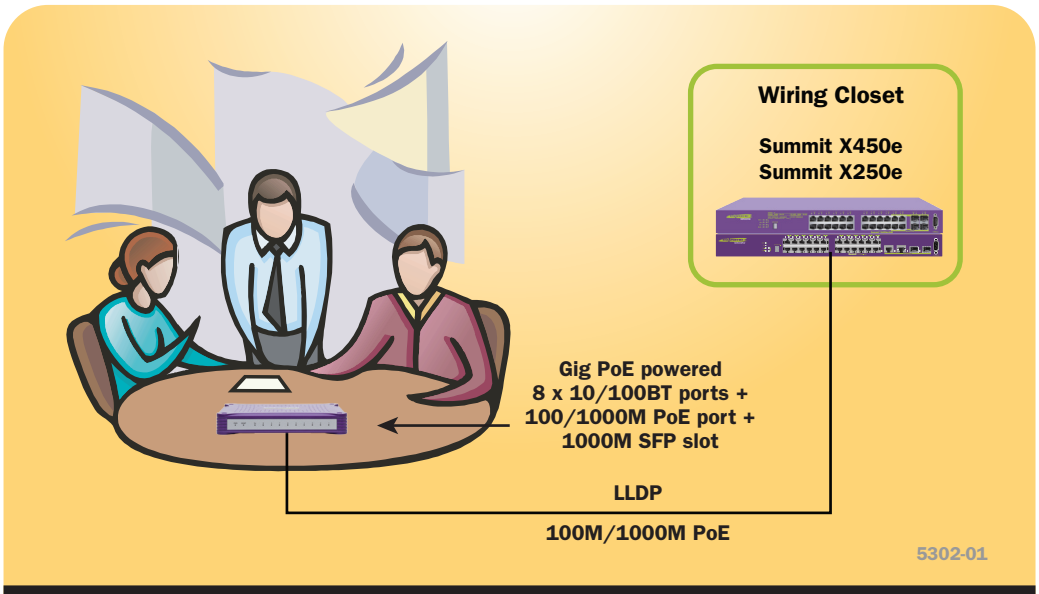

Figure 1: Conference room application with upstream ExtremeXOS PoE switch

Guest VLAN

ExtremeXOS NetLogin includes a Guest VLAN feature. With this feature enabled, if a client connected to a NetLogin-enabled port does not respond to the 802.1x authentication requests from the switch, the port moves to the configured guest VLAN. When combined with MAC-based VLANs the client, not the port, is moved to the guest VLAN. This VLAN can be a "Guest" VLAN with restricted access, such as access only to the public Internet. Restricted access can be enforced using access control lists, routing policies and rate limiting.

Authentication Failure VLAN

When this feature is enabled on a NetLogin-enabled port and a NetLogin client fails authentication, the client is moved to an authentication failure VLAN. This VLAN can be the "Guest" VLAN. This feature is useful if a guest has a client that is 802.1x enabled or when using MAC-based authentication as the guest's client station will fail authentication.

Deployment Examples

With NetLogin enabled on an ExtremeXOS switch such as a member of the Summit® family of products, users connect to the ReachNXT 100-8t port extender and authenticate to the network via 802.1x, Web or MAC and are granted network access once their credentials are validated. All authenticated clients can be placed in one VLAN or each client can be placed in a different VLAN. In order to move clients to specific VLANs the RADIUS server must be configured to return VLAN Vendor Specific Attributes (VSAs). VSAs are values that are passed from the RADIUS server to the switch after successful authentication. VSAs can be used by the switch to configure connection attributes such as security policy, VLAN, and location. The ExtremeXOS switch can then logically assign the client's traffic to the specific VLAN based on the client's MAC address. Thus, users' laptops or other devices can belong to separate VLANs when connected to the ReachNXT 100-8t.

Secured guest access can be granted concurrently to visitors when they connect to the ReachNXT as well (such as in a conference room). For example with 802.1x NetLogin, MAC-based VLANs, Guest VLAN and authentication failure VLAN enabled on the ExtremeXOS switch, guests can be granted segregated network access. When a guest connects their device to the ReachNXT it is moved to the configured Guest VLAN since their client does not respond to an 802.1x authentication request from the ExtremeXOS switch. If the guest's client device happens to be configured and enabled for 802.1x it will fail authentication and will be moved the configured authentication failure VLAN. This guest VLAN can be secured using ACLs to block all traffic destined to internal resources but allow traffic destined to the public Internet. Routing policies can also be configured to forward all traffic from this guest VLAN to a firewall. Visitors would be able to reach the Internet, but unable to access the corporate network. In addition bandwidth can be restricted using bidirectional rate shaping.

In addition to or as an alternative to the authentication failure VLAN method for guest access, a special user account can be created for guests. It can be posted in the conference room or incorporated in the Captive Portal Web page. The guest account can be secured by the RADIUS server to grant access only based on NAS Identifier or NAS IP address or other unique attributes.

Caveats

- If enabling NetLogin on a ReachNXT connected port, ExtremeXOS 12.1 or later is required on the ExtremeXOS switch. The ReachNXT communicates with the ExtremeXOS switch using Layer Link Discovery Protocol (LLDP), which is required for the ReachNXT to fully boot and become active. In order for LLDP frames to be forwarded on a NetLogin-enabled port, egress traffic must be specifically enabled. This is done via the "configure NetLogin port <port> allow egress all-cast" command available in ExtremeXOS 12.1 or later.
- When the "configure netlogin port <port> allow egress all-cast" command is enabled, broadcast and flooded unicast traffic will be forwarded out the port for any VLANs that are configured on the specified port(s).
- All clients connected to the ReachNXT are in the same broadcast domain. When implementing NetLogin and multiple VLANs, flooded and broadcast traffic is still visible to all devices connected to the ReachNXT. Once the traffic reaches the ExtremeXOS switch it is segregated into the appropriate VLANs. Unicast traffic is switched by the ReachNXT according to its address table. Therefore it is not visible by other devices connected to the ReachNXT.

Please refer to chapter 21 of the ExtremeXOS Concepts Guide for more information on configuring NetLogin.

www.extremenetworks.com

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011