X-Authentication-Warning: hepnrc.hep.net: majordom set sender to owner-p8021@hepnrc.hep.net using -f
Received: from xylan.com (postal.xylan.com [208.8.0.248])
by hepnrc.hep.net (8.9.1/8.9.1) with ESMTP id NAA00088
for <P8021@hepnrc.hep.net>; Mon, 7 Jun 1999 13:28:50 -0500 (CDT)
Received: from mailhub.xylan.com by xylan.com (8.8.7/SMI-SVR4 (xylan-mgw 2.2 [OUT]))
id LAA11082; Mon, 7 Jun 1999 11:28:09 -0700 (PDT)
Received: from newman.xylan.com by mailhub.xylan.com (SMI-8.6/SMI-SVR4 (mailhub 2.1 [HUB]))
id LAA16498; Mon, 7 Jun 1999 11:28:09 -0700
Received: from xylan.com ([127.0.0.1]) by newman.xylan.com
(Netscape Messaging Server 3.5) with ESMTP id AAA36A2;
Mon, 7 Jun 1999 11:29:16 -0700
Message-ID: <375C0EC5.9B957385@xylan.com>
Date: Mon, 07 Jun 1999 11:26:13 -0700
From: "Jeff Hayes" <Jeff.Hayes@xylan.com>
Organization: Xylan Corp
X-Mailer: Mozilla 4.04 [en] (Win95; U)
MIME-Version: 1.0
To: Tony Jeffree <tony@jeffree.co.uk>
CC: P8021@hepnrc.hep.net
Subject: 802.1 Minutes (6/2/99)
Content-Type: text/plain; charset=iso-8859-1
Sender: owner-p8021@hepnrc.hep.net
Precedence: bulk
X-MIME-Autoconverted: from 8bit to quoted-printable by hepnrc.hep.net id NAB00092

Tony, these are the minutes from last week's 802.1 interim meeting.

The following are the minutes of the 802.1 groups held on Tuesday, 2 June 1999, in Coeur d'Alene, ID (USA); as taken by Jeff Hayes. Attendance ~ 18.

Call to order 9:00 a.m. (Mick Seaman)

802.1 Agenda (Mick Seaman)

Port-based Network Access Control
P802.1t - .1D maintenance
P802.1u - .1Q maintenance
P802.1w - rapid configuration
P802.1s - multiple spanning tree
P802.1v - protocol-sensitive VLANs

Port-based Network Access

---

* Presentation on market requirements for port-based network access from Jeff Hayes
    - Discussion on value of adding a MAC-based auth option
    - Problem of security on shared hubs
    - Problem of sending ID/pswd clear text over the net
    - Market demand for this feature: conference room, public access areas, etc.

The presentation text is provided below:

IEEE 802.1 - Port-based Network Access Control

1) What?
    Distributed security
    Authenticate users at the switch port
    Once authenticated, operates at LAN speed
    Leverage common authentication systems
    RADIUS
    DIAMETER

- LDAP compliant directory servers
- NOS

2) Why?
- Perimeter security
  - Access control at the edge
- Not all users created equal
  - Trust all; really trust only a few
- Not all networks created equal
  - Some require extra access control measures

3) Applications
- Distributed user authentication
  - Not device
- Edge access control
  - User mobility with campus setting
- Leveraged by single sign-on systems
  - One ID/pswd, entered one-time

4) Market Demand
- User authentication in enterprises
  - Key departments (HR, Finance)
  - Open computing environments (partners, visitors)
- Network ingress security
  - Access control distributed to the edge
- Key verticals are ideal for switch access control
  - Security conscience environments
  - Mobile users
  - Semi-public work environments

5) Key Vertical: University
- Goal authenticated open computing
  - Broad facilities
  - Central campus, satellites & dorms
- Different user types

- Students - dorms, classrooms & library
- Faculty - offices & classes
- Admin - offices

Authenticate into common, open VLAN
Filter between private nets

6) Key Vertical: Medical
Goal patient & research confidentiality
Facilities
- In/out patient hospital
- Research labs

Users
- MDs, nurses, admins
- Research PhDs & techs

Policy
- Authenticate into key subnets
- Filter/firewall internal traffic

7) Key Vertical: Carrier
Goal secure, multi-layer Internet access
Users connect to network
- Via DSL or cable

Users authenticate at the NSP's POP
- RADIUS
- Multiple authorities

One user per switch port
- Access multiple out-sourced services
- Separate billing

8) Key Administration Issues
Ethernet-only ingress; any egress interface
- No authentication needed for inter-switch ports

Configurable on a per port basis
- Not all switch ports must be authenticated ports

Log-off, aging and inactivity timer options

- Re-authenticate according to policy
- Transparent to authentication server type
- Authenticator can request more information before determining the mechanism
- Smart cards, Kerberos, PKI, 1-time pswd, etc.

9) Key Administration Issues (cont)

- Multiple VLAN membership options
  - Some want a MAC-based option = more control
  - Authenticate into authorized VLAN = choice
  - Client does DHCP after authentication
- Mobility
  - Same look & feel regardless of campus location
  - Mixed vendor enviro=common user experience
  - Many users need both non-auth access and auth access, depending on local port

10) Other possible considerations

- Core spec for the authentication process
- Section/Appendix for port-based authentication
  - All or nothing / open or closed
- Section/Appendix for MAC-based authentication
  - VLAN membership control (IP unicast, IP multicast, IPX, AT, etc.)

11) Summary

- Xylan believes a standards-based switch access authentication method is required
- Key verticals markets have expressed a definite need for this capability
- Although port based access may be easier to implement, do not discount the control layer-2 mechanisms offer, Xylan intends to support the approved spec

* Presentation/discussion on the "Port-based Network Access Control PAR" from Paul Congdon
    - "Scope of Proposed Project"
        -Mechanics use existing authentication and authorization enforced on individual ports
        -Encoding of protocols over 802 LANs
        -Bridges/switches will not interpret auth info, modify frames, filter frames
        -802.1q VLAN while not explicitly addressed are not precluded
        -Concern over the hub attached to the switch port
    - "Purpose of Proposed Project"
        -"Allows a network administrator to control bridged forwarding to and from LAN segments of the bridge based on the authenticated state of the port user (ingress port)"
    - 5 criteria discussion
        -General census; needs some additional word-smithing

* Action: propose PAR to 802 executives; give them 30 days; vote on the PAR at the Plenary in July

P802.1t - .1D maintenance (Tony Jeffree)

Review the technical and editorial corrections of 802.1t/D0 document Annex Z that Tony made available on 25 May 1999:

ftp://p8021:-go_wildcats@p8021.hep.net/8021/t-drafts/d0/802-1t-d0.pdf

* Port number priority = 0-240 in multiples of 16 (make it clear what happens when an illegal value is set)
* Bridge priorities = 0-64k in 4k increments
* Rehash the "Path Cost Parameter Values" table but decided to leave the .1D table alone
    -Purpose of the value cost table is to establish network topology

(must track link speeds)
-Implementer can add more controls as deemed necessary
* Current hold time = 1 second; allow no more than 2 messages in a hold_time period

P802.1u - .1Q maintenance (Tony Jeffree)

Review the technical and editorial corrections of 802.1u/D0 document - Annex Z that Tony made available on 25 May 1999.

ftp://p8021:-go_wildcats@p8021.hep.net/8021/u-drafts/d0/802-1u-d0.pdf

P802.1w - Rapid Reconfiguration (Tony Jeffree)

Review the 802.1w D0 document that Tony made available on 25 May 1999.
ftp://p8021:-go_wildcats@p8021.hep.net/8021/w-drafts/d0/802-1w-d0.pdf

* Introductory statement defining what is "Rapid Reconfiguration"
* The change to spanning tree will not obsolete existing versions of spanning tree (grandfather clause)
* Frame misordering and frame duplication sections are key and the text must reflect the details, once formalized
* Reorganized to the Internal Sublayer Service section
* New MAC Status Parameter section
* Default port forwarding (clause 6)
* Diagrams to include more active topology and context examples - backup & ring topology (clause 17)

P802.1s - multiple spanning tree (Alan Chambers)

---

* Presented MST issues and agreements

-Basics
-Operation
-Stuff

* MST configuration protocol (Cisco VTP derivative)
-Few, small messages in steady state
-Few small messages when state changes
-Minimize processing when receiving updates from others

P802.1v - protocol-sensitive VLANs

Brief discussion
Possible leader (Andrew Smith, Extreme Networks) left early to catch a flight
Further discussion planned for July Plenary

Adjourned: 5:15 p.m. (Mick Seaman)

Jeff.Hayes@Xylan.com http://www.xylan.com
Product Manager - Security, QoS, & L3/4 Switching
Phone: 1.801.487.0525 Pager: 1.800.381.0354