IEEE 802.1
Port-based Network Access Control

Jeff Hayes
Product Manager - Xylan
jeff.hayes@xylan.com
Network Access Control

• 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
Network Access Control

• 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
Network Access Control

- **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
Network Access Control

• 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
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

• IP addressing - DHCP
• Filter between private nets
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
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 outsourced services
  - separate billing
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.
Key Administration Issues

• 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
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.)
Summary

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