Identity Management

Piotr Szołkowski

Compelling Portfolio

A portfolio to address the breadth of Ethernet

Ridgeline™

EPICenter®

Management

Summit® WM

Wireless

Sentriant®

Security

ReachNXT™

Port Extender

SummitStack™

Summit X480

Summit X650

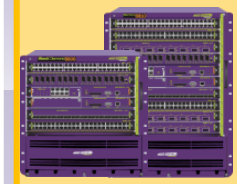
Summit X460

Summit X450a

Summit X250e

Summit X450e

BlackDiamond® 8900 8800 8500



BlackDiamond 10K/12K

BlackDiamond 20K

Summit X150

Summit X350

METRO CORE

DATA CENTER

AGGREGATION

ADVANCED EDGE

VALUE EDGE

10/100 Mb | 1 Gigabit | 10 Gigabit | 40 Gigabit | 10/100 Mb – 10 Gigabit – 40 Gigabit

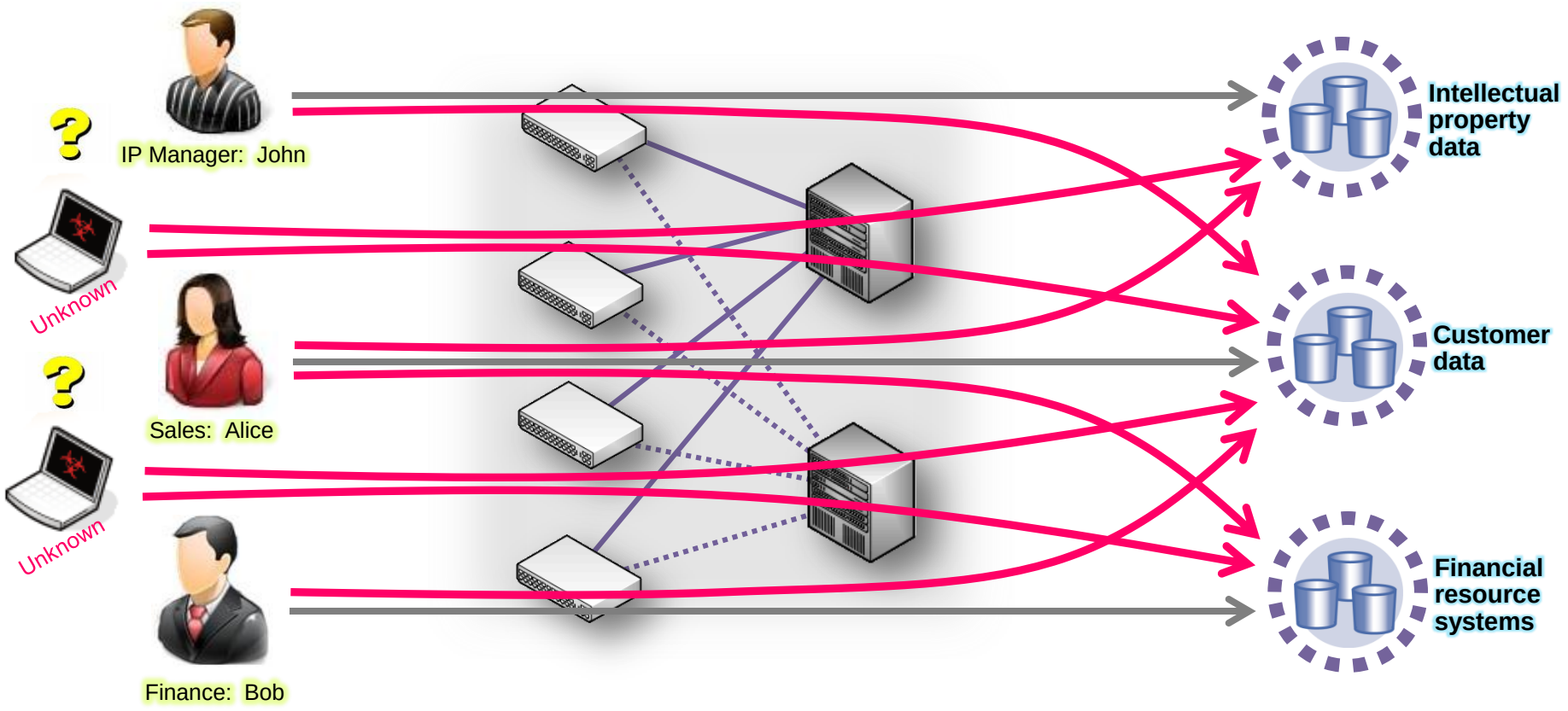
ExtremeXOS® Network Operating System

Network-based Identity and Access Management

Extending security monitoring and provisioning of users to the network for greater control

Traditional IdAM

Identity and Access Management (IdAM) provisioning at the application (i.e. resource) level



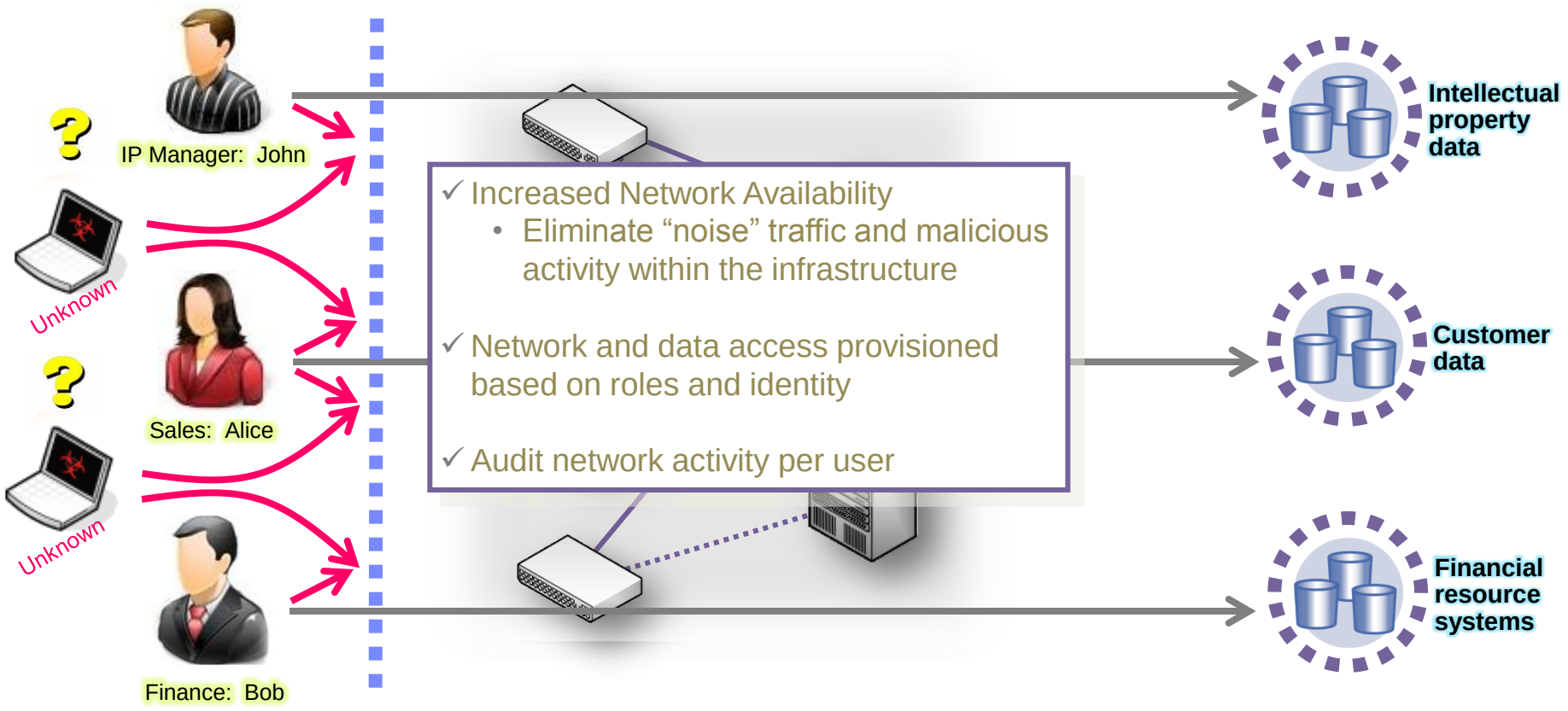
User Community

Network Infrastructure

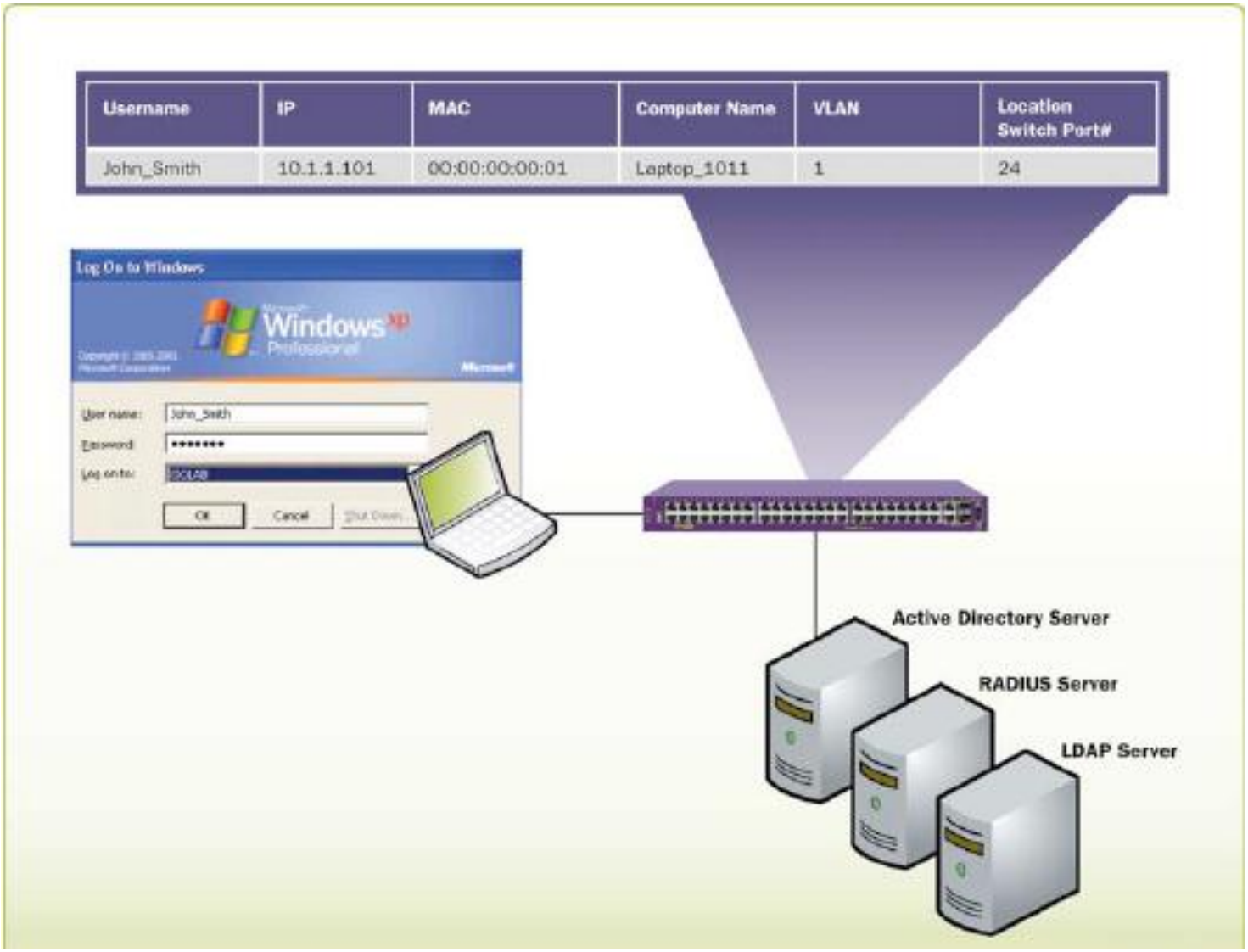
Protected Application / Data Center

Network-based IdAM

Identity and Access Management (IdAM) provisioning at the network and application level with Extreme Networks



Identity Manager



Identity Management Phase 1 – A Recap

In phase 1 (XOS 12.4.1), Identity management primarily monitored users and devices across the network

Users and devices are detected by various means:

- Identities derived from Netlogin, Kerberos and LLDP
  - Netlogin 802.1X Login ID
  - Netlogin Web-based ID
  - Netlogin MAC-radius
  - LLDP-based device identification (e.g. VoIP Phone)
  - Kerberos Snooping: from analyzing Kerberos packet exchange.

  during Windows Active Directory Domain Login.
- Mappings like IPv4 address<->MAC<->port are derived from ARP, FDB, IP Address Security modules.

- Reporting: Location tracking based on username/device name (EPICenter)

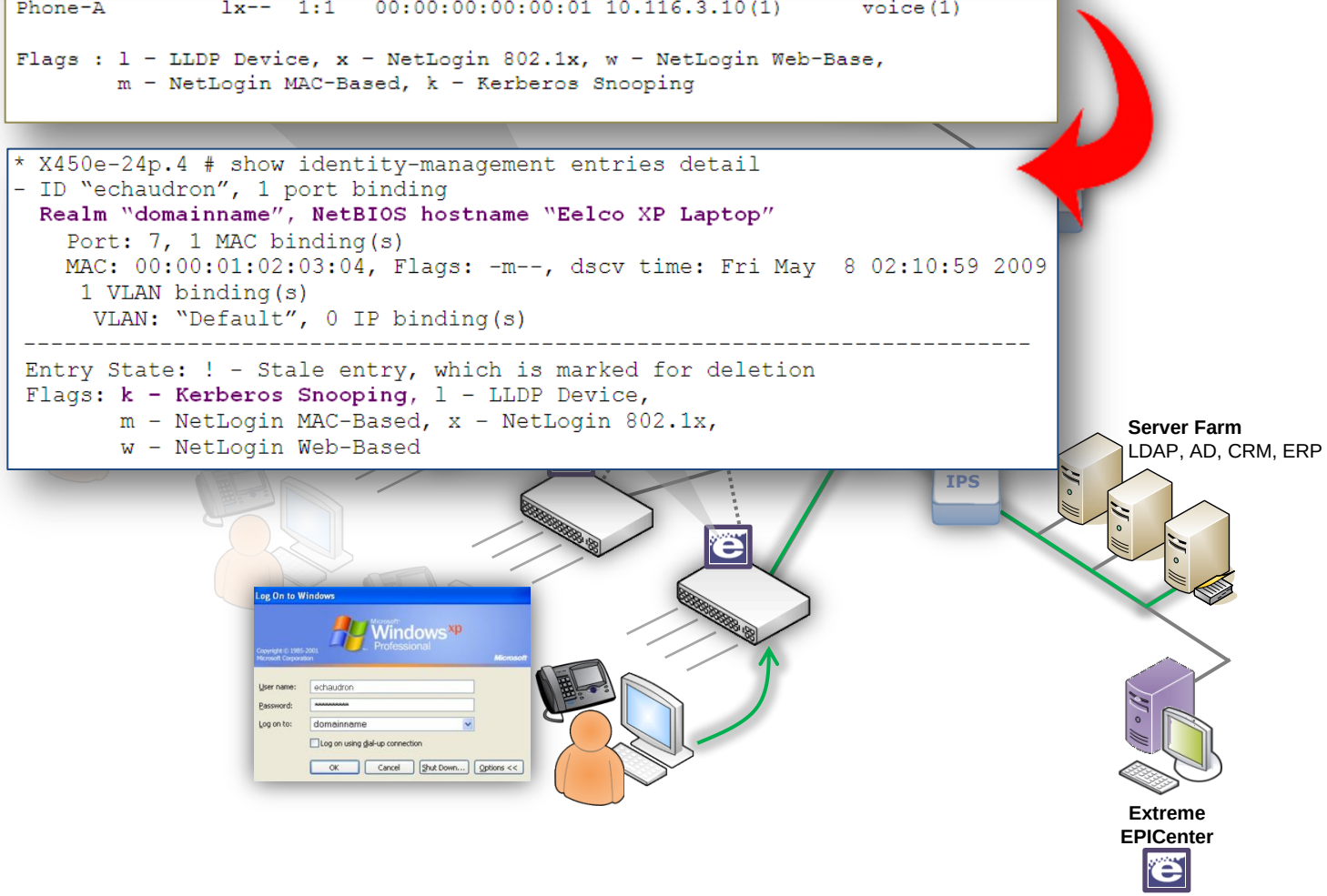
Identity Management Phase 1

```
* X450e-24p.4 # show identity-management entries

ID Name          Auth  Port  MAC               IP                VLAN
-------------------------------------------------------------------------------
psingh           -w--  9:200 00:00:00:00:00:01 255.255.255.255(10) employee(10)
echaudron        --k-  1:1   00:00:00:00:00:01 10.116.3.10(1)      default(1)
Phone-A          lx--  1:1   00:00:00:00:00:01 10.116.3.10(1)      voice(1)

Flags : l - LLDP Device, x - NetLogin 802.1x, w - NetLogin Web-Base,
        m - NetLogin MAC-Based, k - Kerberos Snooping
```

```
* X450e-24p.4 # show identity-management entries detail
- ID "echaudron", 1 port binding
  Realm "domainname", NetBIOS hostname "Eelco XP Laptop"
    Port: 7, 1 MAC binding(s)
    MAC: 00:00:01:02:03:04, Flags: -m--, dscv time: Fri May  8 02:10:59 2009
     1 VLAN binding(s)
      VLAN: "Default", 0 IP binding(s)
 -------------------------------------------------------------------------------
 Entry State: ! - Stale entry, which is marked for deletion
 Flags: k - Kerberos Snooping, l - LLDP Device,
        m - NetLogin MAC-Based, x - NetLogin 802.1x,
        w - NetLogin Web-Based
```



Identity Management Phase 2

Role-policy based user management

- Every identity learnt on the switch is assigned a role
- Dynamic ACLs or policies configured for each role is applied for that identity on the port on which the identity is detected.

How is an identity put under a particular role?

- The administrator can configure user roles and the criteria to put users under that role.
- An LDAP request querying for the attributes of the identity is sent to the LDAP server.
- The identity is placed under the role whose criteria is met by the LDAP attributes received from the server.
- Other than the user configured roles, Identity Manager supports two default roles – authenticated and unauthenticated. Identities which do not fall under any other role will be put under one of these two roles.

LDAP Attributes supported in 12.5.1

List of User LDAP attributes that will be queried :

- Employee ID
- Title
- Email Address
- Department
- Company
- Locality
- State
- Country

LDAP configuration

LDAP servers can be added as both hostnames and IP addresses.

Identity manager can be configured to contact the server securely using SSL.

A username and password credential combination that has read access to the Active Directory has to be configured so that information about the identities can be retrieved.

Also a base LDAP domain name where the users can be searched needs to be configured.

Role Match Criteria

The match criteria for a role can be formulated using a combination of the LDAP attributes and the operators equals(‘==‘), not equals(‘!=‘) and ‘contains’.

Example:

1. create identity-management role “India-Engr” “country==India; AND department==Engineering;” add policy “ind-engr-policy”

2. create identity-management role “US-Marketing” “country==USA; AND “department contains Market” add policy “USMarketPol”

3. create identity-management role “Intl-Marketing” “country!=USA; AND “department contains Market” add policy “IntlMarketPol”.

Role Priority

- Each role can be assigned a priority value. The default value is 255.
- The identities are matched against each role based on the priority.
- If an identity satisfies the match criteria of two or more roles, the identity is placed in the role with lesser priority value.
- For example, if an identity matches both role1 with priority 100 and role2 with priority 200, the identity will be placed in role1.

Role-Policy based User Management

Each role can be assigned a set of policies that will be applied to all identities that are mapped to that role.

A role can be assigned both dynamic ACLs and policies.

The identity's source IP address will be used for applying the dynamic ACLs and policies.

When a dynamic ACL/policy is added to a role, it is immediately installed for all identities mapped to that role.

Effective configuration of the dynamic ACLs and policies will ensure that intruders are avoided at the port of entry on the edge switch itself thereby reducing noise in the network.

Role-Policy based User Management

Role	Internet	Intranet	Mail	CRM/Database	VLAN
Unauthenticated	Yes	No	No	No	Default
Contractor	Yes	Yes	No	No	Default
Employee	Yes	Yes	Yes	Yes	Default

User: John
Role: Employee
Resource Access = Permit All

User: Alice
Role: Contractor
Resource Access = Deny Mail and CRM

User: Bob
Role: Unauthenticated
Resource Access = Internet Only

Active Directory Server
RADIUS Server
LDAP Server

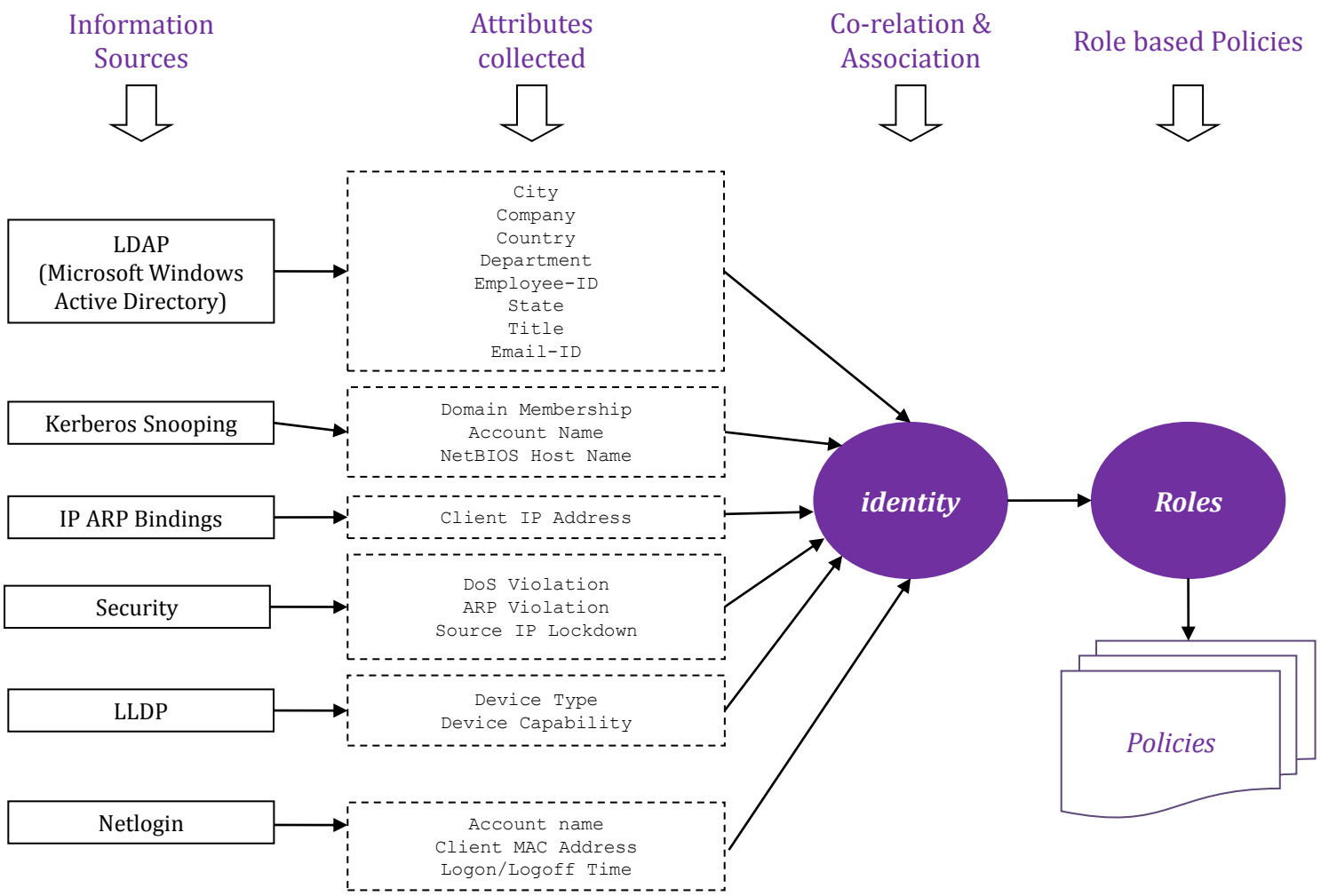
Internet

Intranet

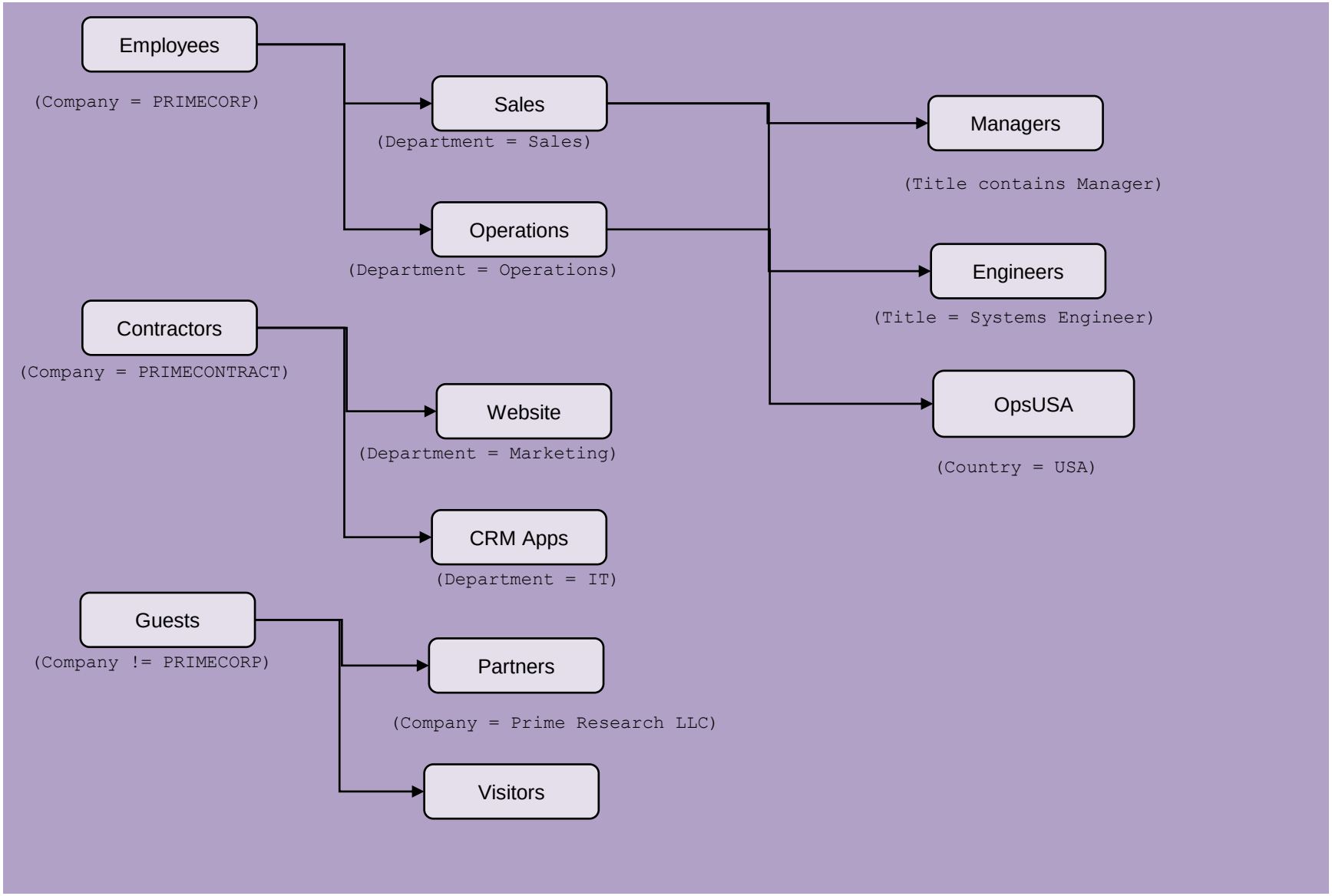
Mail Servers

Data Center

Role-Policy based User Management



Hierarchy of roles



Switch programming

- Script execution
  - Manually via CLI – *load script <file name> {arg1} {arg2} ....*
  - Automatically at given date and time – one time
  - Automatically after given time – one time
  - Automatically from given date time, every defined time – many times
  - Automatically based on events:
    - Device Detect
    - Device Undetect
    - User-Authenticate
    - User-Unauthenticate
    - Identity-Detect
    - Identity-Undetect
    - Identity-Role-Associate
    - Identity-Role-Disassociate
  - Automatically based on ACL counters – CLEAR-Flow