



Workshop Smart OmniEdge

Москва, 11 апреля 2019 г.

Extreme Smart OmniEdge

Pervasive Intelligence



AI/ML
Extensive APIs
Actionable Analytics

Адаптация под Задачи бизнеса



Consistent experience
Hybrid-cloud flexibility
Защита инвестиций

Intrinsically Secure



User security
Device security
Application security

Transforming the **Edge Experience**

Содержание

EVD для сети малого офиса

Построение проводного сегмента сети

Разграничение прав доступа к сетевым ресурсам

Рекомендации Extreme Networks по построению сети



EXTREME VALIDATED DESIGN

Extreme Smart OmniEdge for Primary/Secondary Education

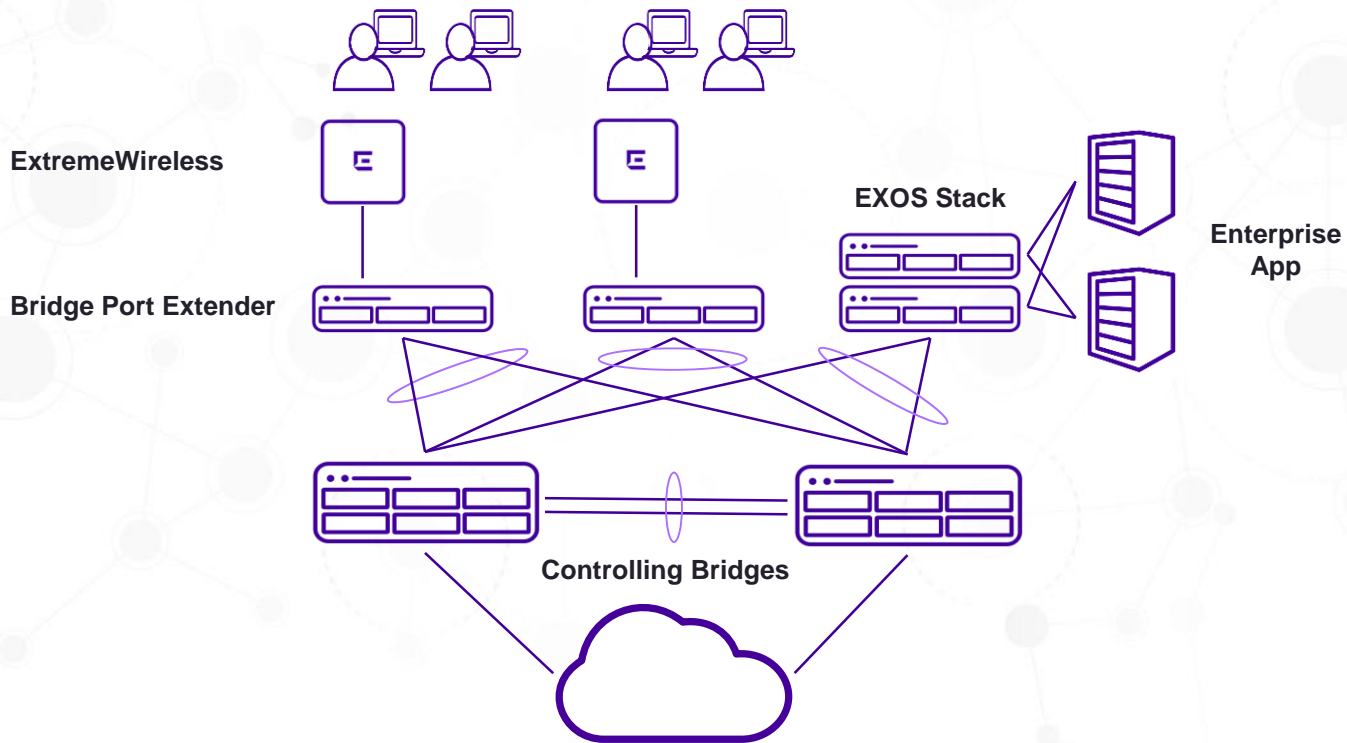
Version 1.1

<https://www.extremenetworks.com/extreme-validated-solutions/>

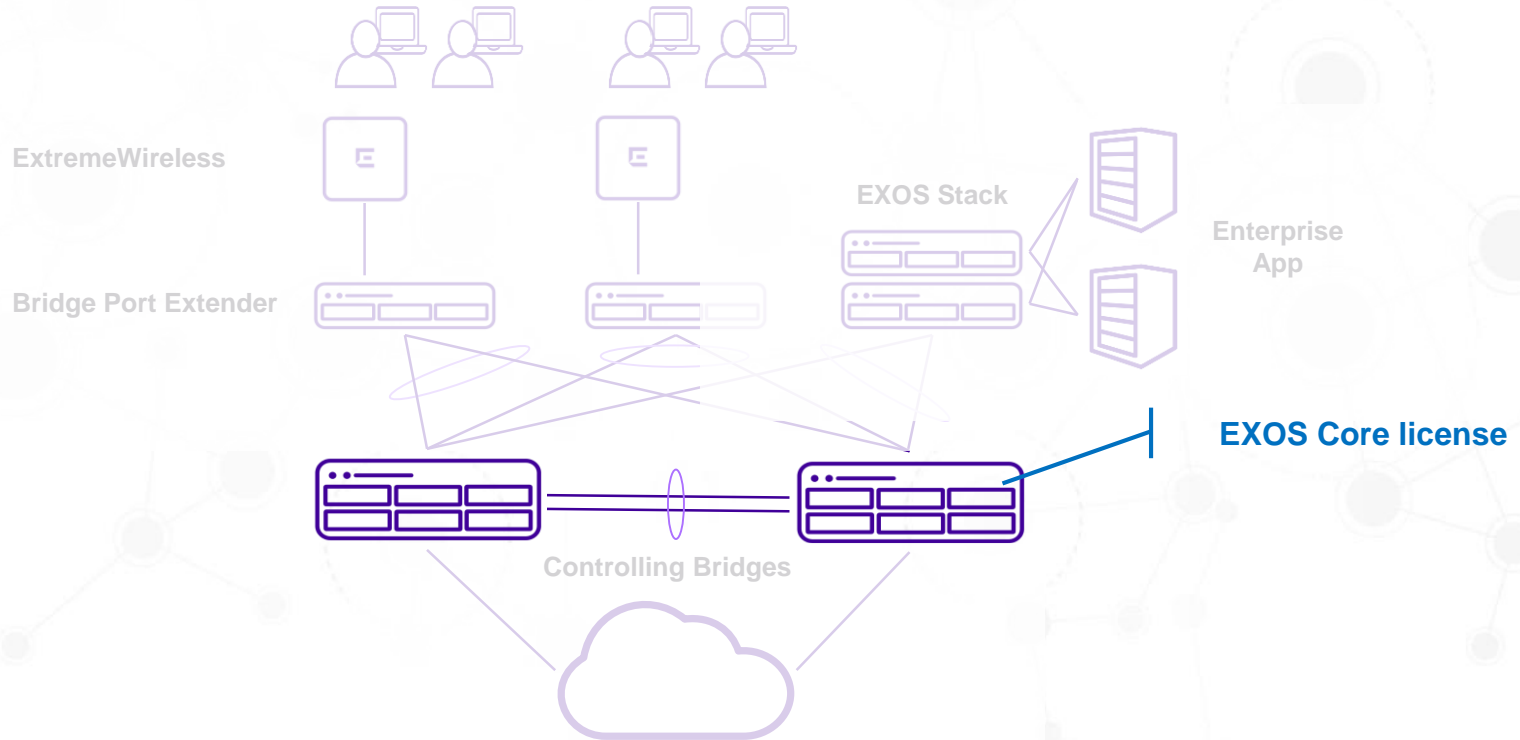


Настройка проводного сегмента сети

Корпоративная сеть связи



Рекомендации по уровню лицензирования EXOS



ZTPStack для автоматической настройки VPEX

ZTPStack предназначен для:

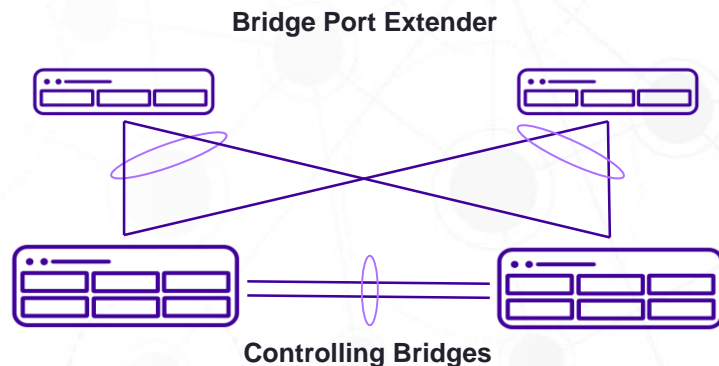
- Включения VPEX режима, если обнаружен подключенный VPE
- Автоматическая настройка MLAG со вторым СВ
- Включение VPEX-autoconfiguration

```
* Slot-1 VPEX X670G2-48x-4q.17 # sh slot
Slots      Type          Configured      State      Ports  Flags
-----
Slot-1     X670G2-48x-4q  X670G2-48x-4q  Operational  64    M
Slot-100   V400-48t-10GE4 V400-48t-10GE4 Operational  52    M
Slot-101   V400-24t-10GE2 V400-24t-10GE2 Operational  26    M

Flags : M - Backplane link to Master is Active
        B - Backplane link to Backup is also Active
        D - Slot Disabled
        I - Insufficient Power (refer to "show power budget")
* Slot-1 VPEX X670G2-48x-4q.18 #
* Slot-1 VPEX X670G2-48x-4q.18 # sh vpeX

Virtual Port Extender: Enabled
Auto-Configuration:   Enabled

Cascade
Port      Slot
=====
1:23      100
100:50    101
* Slot-1 VPEX X670G2-48x-4q.19 #
```



Синхронизация настроек Controlling Bridges

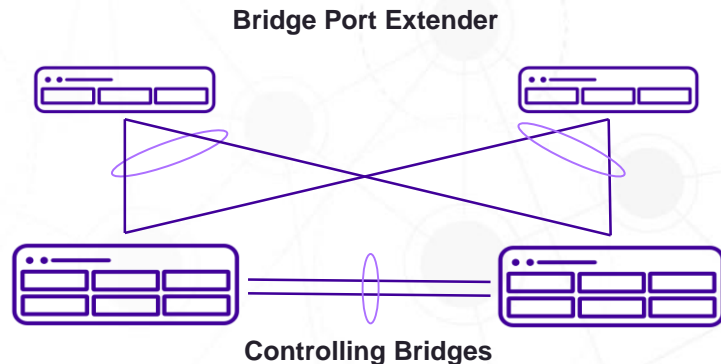
- Все настройки выполняются на одном устройстве
- Команды автоматически копируются на второй коммутатор
- Требуется предварительная настройка MLAG пары
- Может использоваться для настройки других технологий

```
# start orchestration mlag vpex_peer
(orchestration vpex_peer) # enable sharing 1:23 grouping 1:23 lacp
(orchestration vpex_peer) # enable mlag port 1:23 peer vpex_peer id 100
(orchestration vpex_peer) # config vpex port 1:23 slot 100
(orchestration vpex_peer) # enable sharing 100:49 grouping 100:49-50 lacp
(orchestration vpex_peer) # config vpex port 100:49 slot 101
WARNING: This command will remove VLAN membership from the
port 100:49.
Do you want to continue? (y/N) Yes
(orchestration vpex_peer) #
(orchestration vpex_peer) # sh slot
```

Slots	Type	Configured	State	Ports	Flags
Slot-1	X670G2-48x-4q	X670G2-48x-4q	Operational	64	M
Slot-100	V400-48t-10GE4	V400-48t-10GE4	Operational	52	M
Slot-101	V400-24t-10GE2		Booting	26	

Flags : M - Backplane link to Master is Active
B - Backplane link to Backup is also Active
D - Slot Disabled
I - Insufficient Power (refer to "show power budget")

```
(orchestration vpex_peer) #
```



Создание пользовательских VLAN

- Симметричные настройки должны быть сделаны на обоих СВ-коммутаторах
- Допустимо использовать **mlag orchestration** режим для синхронизации настроек
- IP адреса и другие индивидуальные параметры должны настраиваться на каждом устройстве

Добавление VLAN на LACP группы

Включение Bootrelay для работы DHCP сервера

```
create vlan "VLAN_101"  
configure vlan "VLAN_101" description "Wired Users"  
configure "VLAN_101" tag 101  
configure "VLAN_101" add ports 1:45,1:49 tagged  
enable bootrelay ipv4 vlan "VLAN_101" lan VLAN_1900  
  
configure vlan "VLAN_101" add ports 1:1-24 untagged
```

Добавление VLAN на пользовательские порты

Настройка VRRP для пользовательских VLAN

- Симметричные настройки должны быть сделаны на обоих СВ-коммутаторах
- Допустимо использовать *mlag orchestration* режим для синхронизации настроек
- IP адреса и другие индивидуальные параметры должны настраиваться на каждом устройстве

Настройка IP адреса на VLAN

Настройка VRRP группы на VLAN

Controlling Bridge 1

```
configure "VLAN_101" ipaddress 172.16.101.2/24
enable ipforwarding "VLAN_101"
```

```
create vrrp vlan VLAN_101 vrid 101
configure vrrp "VLAN_101" vrid 101 fabric-routing on
configure vrrp "VLAN_101" vrid 101 add 172.16.101.1
configure vrrp "VLAN_101" vrid 101 priority 255
enable vrrp "VLAN_101" vrid 101
```

Fabric-routing включает ответ от ближайшего маршрутизатора в группе

Приоритет для балансировки нагрузки

Настройка Loopback интерфейсов

- Для удаленного управления через XMC
- Для Router-ID в протоколах маршрутизации
- Настраивается на каждом устройстве индивидуально

Controlling Bridge 1

```
create vlan "lo0"  
configure vlan "lo0" tag 1001  
enable loopback-mode vlan "lo0"  
configure vlan "lo0" ipaddress 192.168.200.1 255.255.255.255  
enable ipforwarding vlan "Lo0"
```

Controlling Bridge 2

```
create vlan "lo0"  
configure vlan "lo0" tag 1001  
enable loopback-mode vlan "lo0"  
configure vlan "lo0" ipaddress 192.168.200.2 255.255.255.255  
enable ipforwarding vlan "Lo0"
```

Специальный режим для Loopback интерфейсов

/32 маска для Loopback

Настройка OSPF маршрутизации

Адрес Loopback0 в
качестве Router ID

Анонсируем
пользовательские VLAN

```
configure ospf routerid 192.168.200.1
enable ospf
enable ospf export direct cost 0 type ase-type-1
configure ospf add vlan "lo0" area 0.0.0.0
configure ospf add vlan "VLAN_101" area 0.0.0.0
configure ospf vlan "VLAN_101" authentication encrypted md5 1 my_ospf_key
```

Авторизация соседей

Взаимодействие с RADIUS сервером

- Для авторизации сетевых подключений используется RADIUS сервер
- Настраивается взаимодействие с двумя серверами для отказоустойчивости
- В качестве RADIUS сервера используется ExtremeControl

Controlling Bridge 1

```
configure radius 1 server 192.168.250.253 1812 client-ip 192.168.200.1 VR VR-Default
configure radius 1 shared-secret encrypted "My_Radius_Key"
configure radius-accounting 1 server 192.168.250.253 1813 client-ip 192.168.200.1 VR VR-Default
configure radius-accounting 1 shared-secret encrypted "My_Accounting_Key"
```

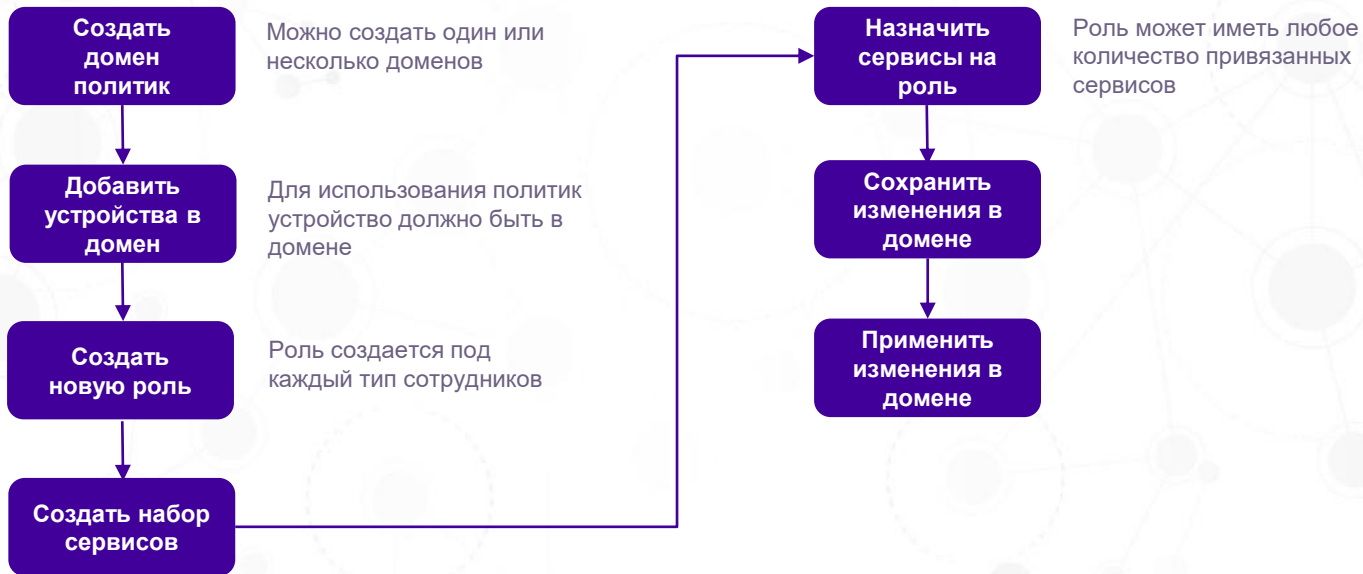
```
enable radius
enable radius mgmt-access
enable radius netlogin
```

```
enable radius-accounting
enable radius-accounting mgmt-access
enable radius-accounting netlogin
```



Разграничение правд доступа пользователей

Алгоритм создания политики доступа



Создание домена политик

- Домен это – контейнер с набором правил
- Устройство может принадлежать только одному домену
- Правила можно импортировать/экспортировать между доменами

Dashboard Policy Access Control End-Syst

Open/Manage Domain(s) Global Domain Settings

Domain: lab.extremenetworks.com

Roles/Services + Devices

Class of Service + Name

VLANs +

Network Resources +

Devices/Port Groups -

Devices Port Groups

by IP ▾

IP (0 devices)

Assign Device(s) to Domain...

Enforce

Verify

Refresh (Rediscover)

Device Authentication Configuration...

Port Authentication Configuration...

Set/Clear Frozen Ports ▸

Assign Device(s) to Domain

Select from supported devices on the left and add them to the current domain list on the right.

Devices

Add Device

Device	Policy Domain
My Network (4 devices)	
All Devices (4 devices)	
ExtremeControl	Unsupported
FabricManager	Unsupported
XCA_LAB	Unassigned
x440-G2	lab.extremenetworks.com
Grouped By (4 devices)	
Wireless Controllers (1 device)	

Current Domain

lab.extremenetworks.com

x440-G2

OK Cancel

Создание роли пользователя

Роль это – контейнер с набором правил, определяющих характеристики трафика пользователей:

- Список разрешенных или запрещенных сетевых сервисов
- QoS маркировка пакетов
- Номер пользовательского VLAN

The screenshot displays the Extreme Networks management console. On the left is a navigation sidebar with categories like Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Tasks, and Administration. The main area shows the 'Roles/Services' configuration page for a domain 'lab.extremenetworks.com'. A 'Create Role...' dialog box is open over the 'Roles' section. In the background, the configuration for the 'NetworkAdmin' role is visible, including fields for Name, Description, TCI Overwrite, and Default Actions. An 'Add/Remove Services' dialog is also present, showing a list of services to be added to the role.

Создание сервиса

- Сервис это – группа правил разрешающих или запрещающих работу определенного сетевого сервиса
- Для составление правил используются информация из L2 или L3 заголовка пакета.
- Стандартные поля
- Точные значения полей или диапазоны значений

The screenshot displays the Extreme Networks management console. The top navigation bar includes 'Dashboard', 'Policy*', 'Access Control', and 'End-S'. The left sidebar has 'Network', 'Alarms & Events', 'Control', 'Analytics', and 'Wireless'. The main area shows 'Roles/Services' configuration. A tree view on the left lists 'Printer', 'Quarantine', 'Server', 'Unregistered', 'VoIP Phone', 'Service Repository', 'Local Services', 'Service Groups', and 'Services'. The 'Services' list includes 'Assessment Services', 'Printing Services', 'Active Directory Services', 'Application Provisioning...', 'Base Services', 'Deny Spoofing and Oth...', 'Deny Unsupported Prot...', and 'Limit Exposure to DoS...'. A 'Create Service...' dialog box is open, showing options: 'Create Service...', 'Create Automated Service...', 'Export All Services to File', and 'Paste'.

Детальное описание сервиса

The screenshot displays the Extreme Networks Policy Manager interface. The left sidebar contains navigation options: Network, Alarms & Events, Control (selected), Analytics, Wireless, Governance, Reports, Tasks, and Administration. The main content area is titled 'Policy' and shows the configuration for the domain 'lab.extremenetworks.com (Modified Locally)'. Under the 'Roles/Services' section, the 'Base Services' category is expanded, listing several services with status indicators (green circles). The 'Rule' table below shows three active rules:

Rule	Summary
Permit- Ethernertype ARP	[Ether : ARP] -> [Permit Traffic]
Permit- IP UDP Port Destination BootP Server	[UDP Dst : BootP Server (67)] -> [Permit Traffic]
Permit- IP UDP Port Destination DNS	[UDP Dst : DNS (53)] -> [Permit Traffic]

Назначение сервиса на роль

The screenshot displays the Extreme Networks configuration interface. The main window shows the configuration for the 'Guest_User' role under the 'Policy' tab. The 'Add/Remove Services' dialog is open, showing a list of services and a selected service.

Role: Guest_User

General | VLAN Egress | Mappings | Port Default Usage

Name: Guest_User

Description:

TCI Overwrite: Disabled

Default Actions

Access Control:	Permit Tra
VLAN:	
Service ID:	
Class of Service:	None
System Log:	Disabled
Audit Trap:	Disabled
Disable Port:	Disabled
AP Aware:	Disabled
HTTP Redirect:	Disabled
Traffic Mirror:	Disabled

Services

Add/Remove Services

All Services & Service Groups

- Create Service
- Active Directory Services
- Application Provisioning - A...
- Application Provisioning - B...
- Application Provisioning - S...
- Assessment Services
- Base Services
- Deny Spoofing and Other A...
- Deny Unsupported Protocol...
- Guest_User
- Limit Exposure to DoS Atta...
- My_App
- My_Service

Selected Services & Service Groups

- Guest_User

OK Cancel

Сохранение изменений в домене и активация

- Изменения в параметрах ролей и политик нужно сохранить
- Применить новые параметры для всех устройств в домене

The screenshot displays the Extreme Networks management interface. The top navigation bar includes 'Dashboard', 'Policy', and 'Access Control'. The 'Policy' tab is active. A dropdown menu is open under 'Open/Manage Domain(s)', showing options: 'Open Domain', 'Lock Domain', 'Save Domain', 'Enforce Domain', 'Enforce Preview...', 'Verify Domain', 'Assign Device(s) to Domain...', 'Create Domain...', 'Delete Domain(s)...', 'Rename Domain...', and 'Import/Export'. The main content area shows the domain 'lab.extremenetworks.com' and various configuration sections like 'Roles/Services', 'Class of Service', 'VLANs', 'Network Resources', and 'Devices/Port Groups'. The 'Control' menu item is highlighted in the left sidebar.

Схема авторизации пользователя

Доступны три способа авторизации пользователей:

- На внешнем RADIUS сервере
- На внешнем LDAP сервере
- С использованием встроенной базы пользователей

The screenshot displays the Extreme Networks management interface. The left sidebar contains navigation options: Network, Alarms & Events, Control (selected), Analytics, Wireless, Governance, Reports, Tasks, and Administration. The main content area is titled 'Access Control' and shows a configuration menu with 'RADIUS Servers' selected. The right-hand panel is the 'RADIUS Servers' configuration window, which includes a table of existing servers and a form to 'Add RADIUS Server'. The form fields are as follows:

RADIUS Server	Auth Port	Acct Port	Timeout Du...	Number of ...
Add RADIUS Server				
RADIUS Server IP:	<input type="text"/>			
Response Window (5-60 sec):	20			
Authentication via XMC or Captive Portal				
Timeout Duration (2-60 sec):	2			
Number of Retries (0-20):	1			
Configuration				
Auth. Client UDP Port:	1812			
<input type="checkbox"/> Proxy RADIUS Accounting Requests				
Accounting Client UDP Port:	1813			
Change Server Shared Secret				
Server Shared Secret:	<input type="text"/>			
Advanced...				
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

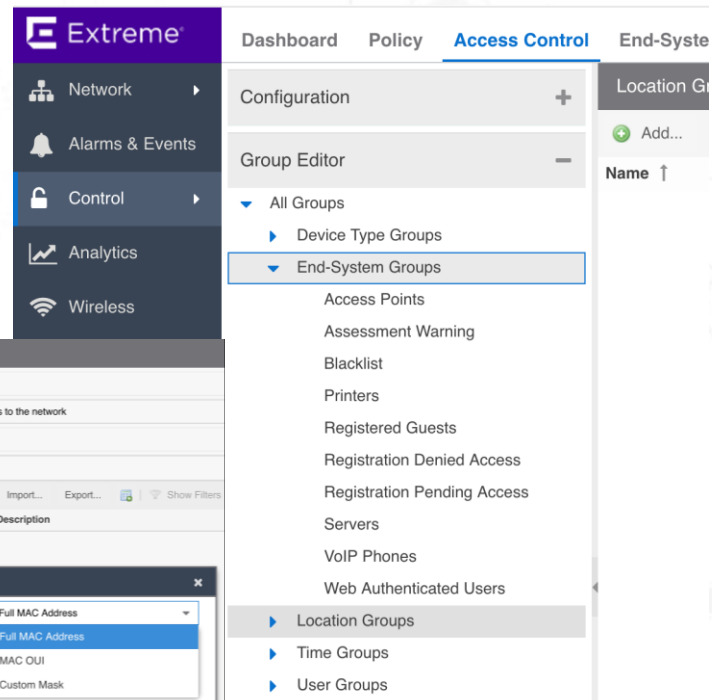
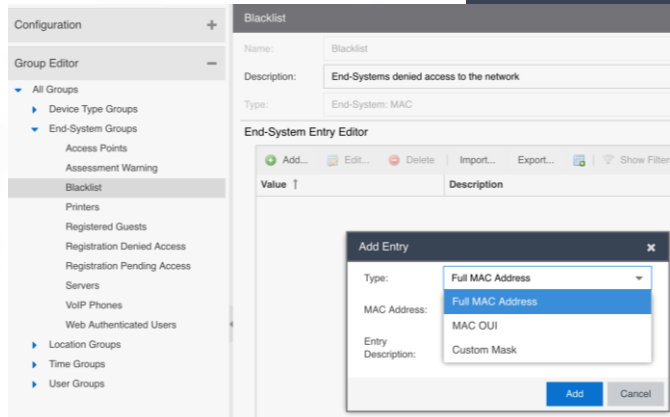
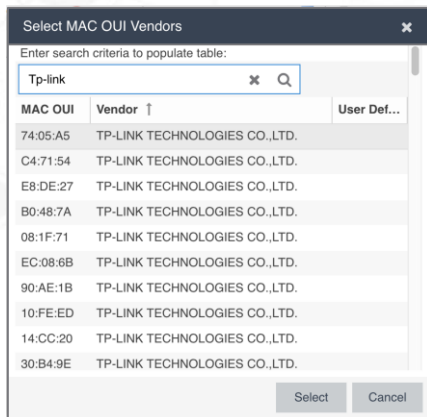
Профайл авторизации

- Набор правил по авторизации абонента
- Определяет назначаемую роль
- Выбор альтернативной роли для аварийного режима
- Ограничения для использования только на отдельной группе устройств
- Включение дополнительных регулярных проверок на соответствие устройства профилю

The screenshot displays the Extreme Networks management console. The left sidebar contains navigation menus for Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Tasks, and Administration. The main content area is titled 'Access Control' and shows a list of profiles under the 'Profiles' section. The 'Administrator NAC Profile' is selected and highlighted. The right-hand pane shows the configuration for this profile, titled 'Access Control Profile - Administrator NAC Profile'. It includes sections for 'Authorization' and 'Assessment'. In the 'Authorization' section, the 'Accept Policy' is set to 'Enterprise User (Administrator)'. Other options include 'Replace RADIUS Attributes with Accept Policy' (checked), 'Use Quarantine Policy' (checked, set to 'Quarantine'), 'Use Failsafe Policy on Error' (unchecked, set to 'Failsafe'), and 'Restrict to End-System Zone' (unchecked, set to 'None'). In the 'Assessment' section, 'Enable Assessment' is unchecked. The 'Assessment Configuration' is set to 'Default', and the 'Assessment Interval' is set to '1' week. There are also checkboxes for 'Hide assessment details and remediation options from end user' (unchecked) and 'Use Assessment Policy' (checked, set to 'Assessing').

Черные и белые списки устройств

- Списки конечных устройств на основе MAC-адресов
- Возможность назначения специальных политик для группы устройств
- На основе полного MAC-адреса
- OUI производителя с возможностью поиска по списку
- Фрагмента MAC-адреса



Типы оконечных устройств

- Категоризация оконечных устройств в зависимости от типа операционной системы
- Возможность назначения разных ролей в зависимости от типа операционной системы
- Встроенные профайлы для большого количества различных типов устройств
- Возможность создавать собственные списки на основе имеющихся профайлов

Extreme

Dashboard Policy **Access Control** End-Systems Reports

Configuration +

Group Editor -

All Groups

- Device Type Groups
 - Android
 - Apple iOS
 - BlackBerry
 - Chrome OS
 - Game Console
 - Linux
 - Mac
 - Windows
 - Windows Mobile
- End-System Groups
- Location Groups
- Time Groups
- User Groups

Windows

Name: Windows

Description: Device Types in Window

Type: Device Type

Device Type Entry Editor

Value ↑	Description
Windows	
Windows 10	
Windows 7	
Windows 8	
Windows 8.1	
Windows 8/ 8.1/ 10/ 2...	
Windows 95	
Windows 98	
Windows NT	
Windows Server 2003	
Windows Server 2008	
Windows Server 200...	
Windows Vista	
Windows Vista/ 7/ 2008	
Windows XP	

Авторизация пользователя

- Упорядоченный список правил
- Просмотр списка сверху вниз до первого совпадения критериев
- Черные и белые списки устройств
- Группы оконечных устройств по типу
- Общее правило для всех в конце списка

The screenshot displays the Extreme Networks management console. The left sidebar contains navigation options: Network, Alarms & Events, Control (selected), Analytics, Wireless, Governance, Reports, Tasks, and Administration. The main content area is titled 'Access Control' and shows a tree view of configurations. Under 'Configurations', 'Rules' is selected, showing a list of rules including 'Blacklist', 'Assessment Warning', 'Access Point', 'Server', 'Printer', and 'VoIP Phone'. The 'Blacklist' rule is highlighted, and its details are shown in a table below.

Ena...	Rule Name	Conditions	Actions
✓	Blacklist	End-System is in Blacklist	Profile: Quarantine NAC Profile Accept Policy: Quarantine
✓	Assessment Warning	End-System is in Assessment Warning	Profile: Notification NAC Profile Accept Policy: Notification
	Access Point	End-System is in Access Points	Profile: Access Point NAC Profile Accept Policy: Access Point
	Server	End-System is in Servers	Profile: Server NAC Profile Accept Policy: Server
	Printer	End-System is in Printers	Profile: Printer NAC Profile Accept Policy: Printer
	VoIP Phone	End-System is in VoIP Phones	Profile: VoIP Phone NAC Profile Accept Policy: VoIP Phone

Accept Policy - Role Details: Select a row...

Настройка авторизации на коммутаторе

The screenshot displays the Extreme Networks NetSight Administrator web interface. The main navigation menu on the left includes sections for Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, Tasks, and Connect. The current view is under the 'Policy' tab, specifically in the 'Authentication' sub-tab. A modal dialog box titled 'Port Authentication Status' is open, presenting the following options:

- Disable authentication on all ports
- Disable authentication on interswitch ports
- Select ports on which to disable authentication
- Do not disable authentication on any ports

The dialog also includes an 'Apply' button and 'OK'/'Cancel' buttons. In the background, the 'Authentication' configuration page is visible, showing settings for 'Auth Type Precedence (High->Low): X/WEB/MAC/CEP', 'Re-Auth Timeout Action: N/A', and 'RFC3580 VLAN Authorization: Disabled'. The status bar at the bottom indicates the user is 'NetSight Administrator/root' and the system was last updated on 2018/11/06 16:22:55.

Настройка авторизации на коммутаторе

Dashboard Policy Access Control End-Systems Reports

Open/Manage Domain(s)
Domain: Group1Wired

Roles/Services
Class of Service
VLANs
Network Resources
Devices/Port Groups

Devices Port Groups
by IP
IP (1 device)
10.10.10.x (1 device)
X440-G2-Group1

Enforce Auto Collapse Panel

MAC Authentication Settings

Disable authentication on the following port(s):

Name	Default Role	Device IP	Alias	Stats	Port T
10.10.10.2					
Switch [16 ports]					
<input checked="" type="checkbox"/> 1:1		10.10.10.2		✓	Acco
<input checked="" type="checkbox"/> 1:2		10.10.10.2		✓	Inter
<input checked="" type="checkbox"/> 1:3		10.10.10.2		✓	Inter
<input checked="" type="checkbox"/> 1:4		10.10.10.2		✓	Acco
<input checked="" type="checkbox"/> 1:5		10.10.10.2		✓	Acco
<input checked="" type="checkbox"/> 1:6		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:7		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:8		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:9		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:10		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:11		10.10.10.2		✓	Acco
<input checked="" type="checkbox"/> 1:12		10.10.10.2		✓	Inter
<input type="checkbox"/> 1:13		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:14		10.10.10.2		✓	Acco
<input type="checkbox"/> 1:15		10.10.10.2		✓	Acco

precedence (High->Low): XWEB/MAC/CEP

about Action: N/A

LAN Authorization: Disabled

OK Cancel

[NetSight Administrator/root] Last Updated: 2018/11/06 16:22:55 Uptime: 0 Days 01:38:18

Operations*

Настройка авторизации на коммутаторе

The screenshot displays the Extreme Networks configuration interface. The main window is titled "Port Authentication Configuration" and is divided into three tabs: "1. Device Selection", "2. Port Selection", and "3. Port Configuration". The "3. Port Configuration" tab is active, showing various authentication settings. A note states: "Note: EXOS devices do not support Force Auth/Unauth modes." The settings include:

- Authentication Mode: Authentication Optional (Active / Default Role)
- Port Mode (Auth / Unauth Behavior): Enabled
- MAC Auth Status: Enabled
- 802.1X Auth Status: Enabled
- Web-Based Auth Status: Enabled
- Quarantine Auth Status: Enabled
- Auto Tracking Auth Status: Enabled

Below these settings are expandable sections for "RFC3580 VLAN Authorization", "Login Settings", "Automatic Re-Authentication", and "Authenticated User Counts". At the bottom of the configuration window are buttons for "< Back", "Next >", "Finish", and "Cancel".

The interface also shows a sidebar with navigation options like Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, and Tasks. The status bar at the bottom indicates the user is [NetSight Administrator/root] and the system has been last updated on 2018/11/06 16:33:44 with an uptime of 0 Days 01:38:18.

Отчет по подключенным пользователям

The screenshot displays the Extreme Networks management console. The top navigation bar includes 'Dashboard', 'Policy', 'Access Control', 'End-Systems', 'Reports', and 'End-System Details - pc-tosh-1'. A sidebar on the left contains menu items: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, Tasks, and Connect.

The main content area shows a table of connected end-systems with the following columns: MAC Address, MAC OUI Vendor, Host Name, Device Fam..., Device Type, User Name, Switch IP, Switch Nickname, Switch Port, Policy, and Authorization. The table contains five rows of data.

Below the table is a pagination control showing 'Page 1 of 1' and 'Displaying 1 - 5 of 5'. The section 'End-System Events and Health Results' includes a 'Refresh' button and search filters. It contains a table with columns: Health, Time Stamp, Access Control..., Profile, IP Address, MAC Address, User Name, Host Name, Device Fam..., Device Type, State Description, and Extended St.

MAC Address	MAC OUI Vendor	Host Name	Device Fam...	Device Type	User Name	Switch IP	Switch Nickname	Switch Port	Policy	Authorization
30:3A:64:00:7C:06	Intel Corporate	pc-tosh-1	Windows	Windows 8/...	seIstudent1	10.10.10.12	ewc-group1.se.c...	Group1-AP3...	Student	Filter-Id=Enterasys.v...
54:EE:75:30:94:22	Wistron InfoCo...	kconway-PC1	Windows	Windows 8/...		10.10.10.2	X440-G2-Group1	1:7	IoT Device	Filter-Id=Enterasys.v...
C0:BD:D1:80:3F:08	SAMSUNG ELE...	android-a1ca9a90b...	Android	Android		10.10.10.12	ewc-group1.se.c...	Group1-AP3...	IoT Device	Filter-Id=Enterasys.v...
C4:54:44:6B:F7:2C	QUANTA COM...	pc-tosh-1	Windows	Windows 8/...	staff1	10.10.10.2	X440-G2-Group1	1:7	Corporate	Filter-Id=Enterasys.v...
DA:84:66:C3:A3:18			Amazon Kindle	Amazon Kindle		10.10.10.12	ewc-group1.se.c...	Group1-AP3...	Unregistered	Filter-Id=Enterasys.v...

Health	Time Stamp	Access Control ...	Profile	IP Address	MAC Address	User Name	Host Name	Device Fam...	Device Type	State Description	Extended St
✓	2018/11/14 14:24:06	10.10.10.11	Student Prof...	10.10.10.109	30:3A:64:00:7C:06	seIstudent1	pc-tosh-1	Windows	Windows 8/...	No Error	
✓	2018/11/14 14:24:06	10.10.10.11	Student Prof...		30:3A:64:00:7C:06	seIstudent1	pc-tosh-1	Windows	Windows 8/...	This end-system ...	No Error
✓	2018/11/14 14:24:05	10.10.10.11	Student Prof...		30:3A:64:00:7C:06	seIstudent1	pc-tosh-1	Windows	Windows 8/...	No Error	
✓	2018/11/14 14:24:05	10.10.10.11	Student Prof...		30:3A:64:00:7C:06	seIstudent1	pc-tosh-1	Windows	Windows 8/...	Resolving	
✓	2018/11/14 14:23:12	10.10.10.11	Corporate Pr...	10.10.10.109	30:3A:64:00:7C:06	seIstaff1	pc-tosh-1	Windows	Windows 8/...	No Error	
✓	2018/11/14 14:23:12	10.10.10.11	Corporate Pr...		30:3A:64:00:7C:06	seIstaff1	pc-tosh-1	Windows	Windows 8/...	This end-system ...	No Error

At the bottom of the interface, there is a status bar with the text: [NetSight Administrator/root] Last Updated: 2018/11/14 14:10:52 Uptime: 0 Days 03:54:31. On the right side, there are system icons and a notification area showing 'Operations*' with a red indicator.

Детальная информация по пользователю

The screenshot displays the 'End-System Details - pc-tosh-1' page in the Extreme Networks NetSight interface. The page is organized into several sections around a central fingerprint icon representing the device. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Governance, Reports, Administration, Tasks, and Connect. The top navigation bar includes Dashboard, Policy, Access Control, End-Systems, Reports, and End-System Details - pc-tosh-1. The main content area is divided into sections: Access Profile, Access Control, Custom Data, Physical Device Identity, Location, Activity, Access Type, Top Applications, Device Family, Health, and Registration. A central fingerprint icon is surrounded by various icons representing different system components and data points.

Access Profile
End-System | End-System Events | Health Results

Access Control
User Name: se:student1
AuthType: 802.1X
State: ACCEPT
Policy: Student
Profile: Student Profile (Auto)

Access Type
AP: 1648Y-1019200000
Port Alias: GP18021x
AP Port: Group1-AP3935i (D8-84-66-7B-8B-91)

Custom Data
None

Physical Device Identity
30.3A.64.00.7C.06
10.10.10.109
pc-tosh-1

Location
Zone:
10.10.10.12/Group1-AP3935i GP18021x
Default
Access Control Engine/Source IP: 10.10.10.11

Activity
Last seen 11/14/2018 02:24:06 PM
First seen 11/14/2018 12:25:52 PM

Top Applications
No Data

Device Family
Windows
Windows 8/ 8.1/ 10/ 2012

Health
Risk: No Data
Total Score: No Data
Last Scan: No Data

Registration
State: Not Registered

[NetSight Administrator/root] Last Updated: 2018/11/14 14:10:52 Uptime: 0 Days 03:54:31



EXTREME
NOW

WORLD TOUR