



**Session VI**

**Security, ATM, and  
IP Features**

**CISCO SYSTEMS**

3304  
1261\_05\_2000\_c1\_Sec6 © 2000, Cisco Systems, Inc. 1



**Session VI**

**Security**

**Cisco.com**

3304  
1261\_05\_2000\_c1\_Sec6 © 2000, Cisco Systems, Inc. 2

# Security Topics

- **Using IP access lists**
- **Advanced IP access list example**
- **AAA example**
- **Catalyst security**
- **Preparation and Implementation**

# Using IP Access Lists

## Two types: basic and extended

```
access-list 2 permit 1.1.1.0 0.0.0.255
```

```
access-list 100 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0 eq 23
```

## List elements are applied in order

```
access-list 102 deny ip host 1.1.1.1 any
```

```
access-list 102 permit ip host 1.1.1.1 any
```

# Using IP Access Lists (Cont.)

## Implicit deny at end of list

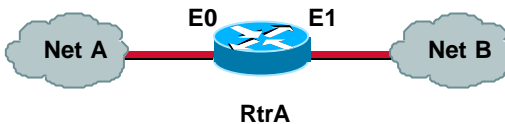
```
access-list 100 permit tcp host 1.1.1.1 any
```

```
access-list 100 permit tcp host 1.1.1.1 any  
access-list 100 deny ip any any
```

## Applied *inbound* or *outbound*

```
serial 0  
ip access-group 10 in
```

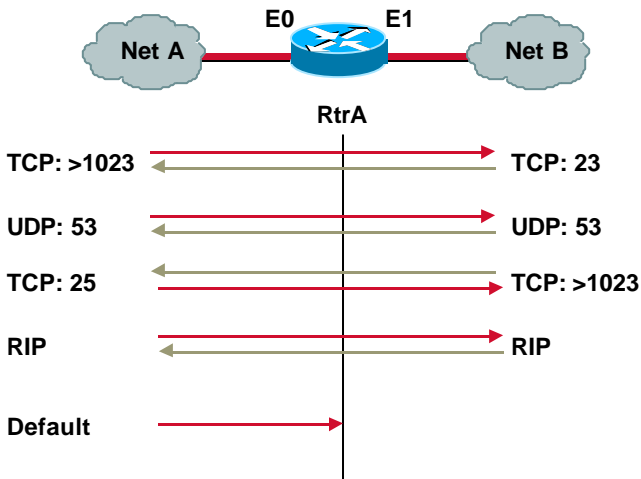
# Access List Example



Apply an outgoing IP access list on ethernet 1 of RtrA such that:

- Telnet sessions originating on net A are allowed
- DNS traffic is allowed
- SMTP sessions originating on net B are allowed
- Routing protocol traffic is permitted
- All other traffic is denied

## Access List Example (Cont.)



## Access List Example (Cont.)

```
interface Ethernet 0
 ip access-group 100 out
 !
 !
 access-list 100 permit tcp any any eq 23
 access-list 100 permit udp any any eq 53
 access-list 100 permit tcp any any eq 25 established
 access-list 100 permit udp any any eq rip
```

(The last line is not strictly necessary here.)

## Debugging Access Lists

***show access-lists*** can provide traffic information on ACL's:

```
RtrA#sh access-lists
Extended IP access list 100
  permit tcp any any eq telnet (10 matches)
  permit udp any any eq domain
  permit tcp any eq smtp any established (1 match)
  permit udp any any eq rip
```

## Debugging Access Lists (Cont.)

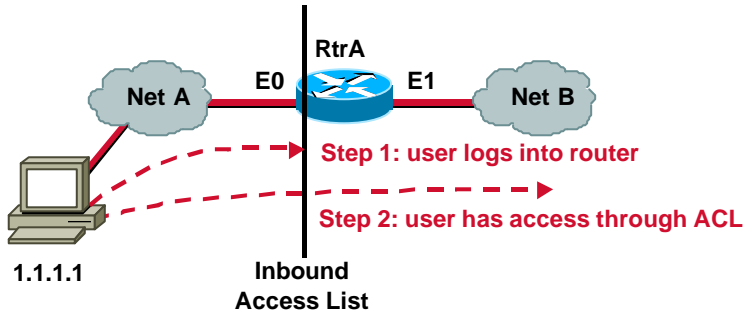
Adding the ***log*** keyword provides more information.

```
access-list 100 permit tcp any any eq telnet log
access-list 100 permit udp any any eq domain log
access-list 100 permit tcp any eq smtp any established log
access-list 100 permit udp any any eq rip log
access-list 100 deny ip any any
```

```
%SEC-6-IPACCESSLOGP: list 100 permitted tcp 1.1.1.1(11003) ->
4.4.4.4(23), 1 packet
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 1.1.1.1 -> 4.4.4.4
(8/0), 5 packets
```

# ACL Feature - Lock-and-Key

Allows a specific user to gain access through an ACL.



## Lock-and-Key (Cont.)

```
hostname RtrA
!  
username fred password 0 cisco
!  
interface Ethernet0  
ip address 1.1.1.2 255.255.255.0  
ip access-group 120 in  
!  
access-list 120 permit tcp host 1.1.1.1 host 1.1.1.2 eq telnet  
access-list 120 permit udp any any eq rip  
access-list 120 dynamic fredlist permit tcp host 1.1.1.1 any eq 23  
!  
line vty 0 4  
login local  
autocommand access-enable
```

# AAA Example

Use RADIUS for default ppp authentication

Try TACACS+, then local for the ISDN link

Authentication server address and key

```
hostname RtrA
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default radius
aaa authentication ppp isdn tacacs+ local
enable password cisco
!
username RtrB password 0 cisco
!
interface BRI0
ip address 138.1.15.2 255.255.255.252
encapsulation ppp
(commands deleted)
ppp authentication chap isdn
!
tacacs-server host 2.2.2.2
tacacs-server key tacacskey
radius-server host 2.2.2.3 auth-port 1645 acct-port 1646
radius-server key radiuskey
```

Enable AAA commands

Use local authentication for access to the router

Local authentication

# Catalyst Port Security

**A Catalyst can be configured to only permit certain MAC addresses on a port.**

```
set port security 2/5 enable 00-0c-22-22-33-33
```

## Catalyst Port Security (Cont.)

Console> (enable) sh port security

Port	Security	Secure-Src-Addr	Last-Src-Addr	Shutdown	Trap	IfIndex
1/1	disabled			No	disabled	3
1/2	disabled			No	disabled	4
2/1	disabled			No	disabled	10
2/2	disabled			No	disabled	11
2/3	disabled			No	disabled	12
2/4	disabled			No	disabled	13
2/5	enabled	00-0c-22-22-33-33	00-30-80-60-ea-40	Yes	disabled	14
2/6	disabled			No	disabled	15

## Preparation Suggestions

- **Know some standard port numbers and protocol behaviors**
- **Practice using access lists you can actually test**

# Preparation Suggestions (Cont.)

## References

[http://www.cisco.com/warp/public/700/tech\\_configs.html#SECURITY](http://www.cisco.com/warp/public/700/tech_configs.html#SECURITY)

<http://www.cisco.com/warp/public/707/index.shtml>

Designing Network Security (Kaeo, Cisco Press)

Enhanced IP Services for Cisco Networks (Lee, Cisco Press)

CiscoCD - Internetworking Design Guide - Security

CiscoCD - Configuration and Command References

# Implementation Suggestions

- **Draw a diagram showing required traffic through the ACL**
- **Watch the order of list elements, and the logic**
- **If all or part of the list can be tested, make sure you do!**
- **Check routing after applying the list.**

## Implementation Suggestions (Cont.)

**Don't forget the "deny all" at the end of the list.**

5.1 Deny all IP traffic to host 1.1.1.1

**Incorrect:**      `access-list 100 deny ip any host 1.1.1.1`

**Correct:**        `access-list 100 deny ip any host 1.1.1.1`  
`access-list 100 permit ip any any`



**Questions?**



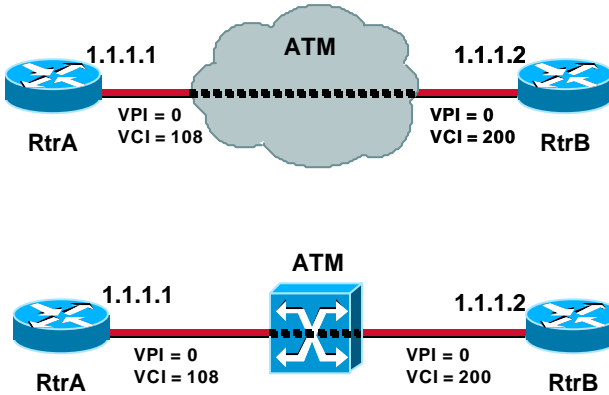
# Session VI

## ATM

## ATM Topics

- **Basic ATM scenarios**
  - PVC - based**
  - Classical IP-over-ATM**
  - LANE**
- **ATM Feature Example**

# PVC Scenario



# PVC Scenario (Cont.)

## End-station configuration example.

```
hostname RtrA
!  
interface ATM3/0  
no ip address  
!  
interface ATM3/0.1 point-to-point  
ip address 1.1.1.1 255.255.255.0  
pvc 0/108  
protocol ip 1.1.1.2  
broadcast  
encapsulation aal5snap
```

**PVC attributes** (points to pvc 0/108)

**Define VPI/VCI values for PVC** (points to 0/108)

**IP address for other side of PVC** (points to 1.1.1.2)

# PVC Scenario (Cont.)

## Verifying PVC setup.

RtrA#show atm vc

Interface	Name	VPI	VCI	Type	Encaps	SC	Peak Kbps	Avg/Min Kbps	Burst Cells	Sts
3/0.1	1	0	108	PVC	SNAP	UBR	155000			UP

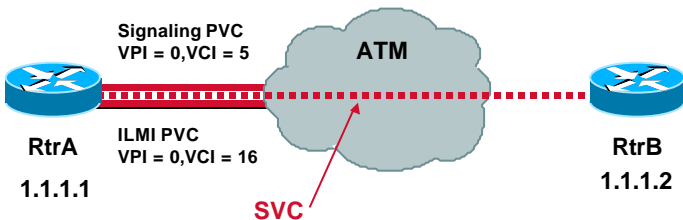
# ATM SVC Setup

NSAP Address: 47.009181000000001007386901.777777777777.00

Prefix

End Station ID

Selector  
Byte

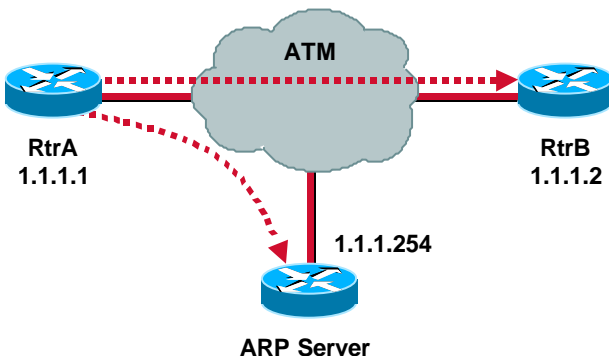


## ATM SVC Setup (Cont.)

- Using SVC's requires the signalling and ILMI PVC's
- Station addressing uses 20-byte NSAP addresses
- Use *show atm ilmi-status* to check ILMI
- Use *debug atm sig-events* to check signalling

## Classical IP- over- ATM

- Step 1: RtrA wants to ping 1.1.1.2
- Step 2: RtrA asks ARP server for NSAP matching 1.1.1.2
- Step 3: RtrA creates SVC to RtrB's NSAP



# Classical IP-over-ATM (Cont.)

## End-station configuration example.

```
interface ATM3/0
no ip address
pvc 0/5 qsaal
pvc 0/16 ilmi
!
!
interface ATM3/0.1 multipoint
ip address 1.1.1.1 255.255.255.0
atm esi-address 777777777777.00
atm arp-server nsap 47.0091810000000001007386901.555555555555.00
```

Signalling and ILMI PVC's

ESI for this end-station

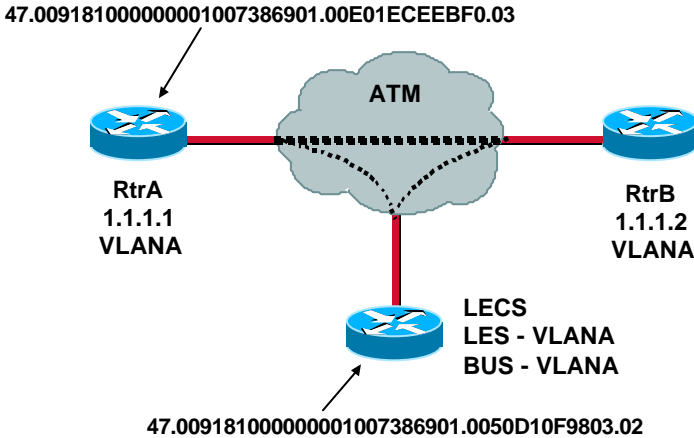
Full NSAP of arp server

# Classical IP-over-ATM (Cont.)

## Checking end-station connectivity.

```
RtrA#show arp
Protocol Address      Age (min) Hardware Addr  Type  Interface
Internet 1.1.1.2           0    0 / 55         ATM   ATM3/0.1
Internet 1.1.1.1           0    0 / 54         ATM   ATM3/0.1
```

# LAN Emulation (LANE)



# LAN Emulation (Cont.)

## End-station configuration example.

```
hostname RtrA
!  
interface ATM3/0  
no ip address  
pvc 0/5 qsaal  
pvc 0/16 ilmi  
!  
interface ATM3/0.1 multipoint  
ip address 1.1.1.1 255.255.255.0  
lane client ethernet VLANA
```

Joins end-station as LANE client

# LAN Emulation (Cont.)

## Verifying LANE client connectivity.

RtrA#**show lane**

LE Client ATM3/0.1 ELAN name: VLANA Admin: up State: operational

Client ID: 2 LEC up for 17 hours 53 minutes 55 seconds

Join Attempt: 1

HW Address: 00e0.1ece.ebf0 Type: ethernet Max Frame Size: 1516

ATM Address: 47.00918100000001007386901.00E01ECEEBF0.03

VCD	rxFrames	txFrames	Type	ATM Address
0	0	0	configure	47.007900000000000000000000.00A03E000001.00
17	1	27	direct	47.009181000000001007386901.0050D10F9803.02
18	46	0	distribute	47.009181000000001007386901.0050D10F9803.02
19	0	15014	send	47.009181000000001007386901.0050D10F9804.02
20	28958	0	forward	47.009181000000001007386901.0050D10F9804.02

# ATM Feature Example

## Setting the Service Class of a PVC using the VC-Class mechanism.

```
hostname RtrA
!
interface ATM3/0.1 point-to-point
ip address 1.1.1.1 255.255.255.0
pvc 0/108
  class-vc vclass ← Apply vc-class to PVC
  protocol ip 1.1.1.2
  encapsulation aal5snap
!
vc-class atm vclass ← vc-class setting service parameters
abr 1000 0
```

# Preparing and Implementing ATM

- **An ATM switch is required to practice SVC-based scenarios. The switch can also be used for various server functions in a test setup.**
- **Classify a test question as a PVC, Classical IP-over-ATM, or LANE question before you start.**

# Preparing and Implementing ATM (Cont.)

## References

**ATM Resource Library, Volumes 1, 2 and 3 (Black, Prentice Hall)**

**<http://www.cisco.com/warp/public/121/index.shtml>**

**CiscoCD - Internetworking Design Guide - ATM**

**CiscoCD - Configuration and Command References**



**Questions?**



**Session VI**

**IP Features**

# IP Features

- **Network Address Translation (NAT)**
- **Domain Name Service (DNS)**
- **Hot Standby Routing Protocol (HSRP)**
- **Dynamic Host Control Protocol (DHCP)**
- **Network Time Protocol (NTP)**
- **HTTP**

# IP Features NAT

- **Network Address Translation (NAT)**
- **NAT allows an organization with nonglobally routable addresses to connect to the Internet by translating those addresses into globally routable address space**

# IP Features NAT

- **NAT uses the following definitions:**
  - **Inside local address**---The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider
  - **Inside global address**--- A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world
  - **Outside local address**---The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from address space routable on the inside
  - **Outside global address**---The IP address assigned to a host on the outside network by the host's owner. The address was allocated from globally routable address or network space

# IP Features NAT

- **Dynamic Inside Source Translation Example:**
  - This example translates all source addresses passing access list 1 (having a source address from 192.168.1.0/24) to an address from the pool named net-208. The pool contains addresses from 171.69.233.208 to 171.69.233.233

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask 255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

# IP Features NAT

## • Overloading Inside Global Addresses Example

- The following example creates a pool of addresses named net-208. The pool contains addresses from 171.69.233.208 to 171.69.233.233. Access list 1 allows packets having the source address from 192.168.1.0 to 192.168.1.255. If no translation exists, packets matching access list 1 are translated to an address from the pool. The router allows multiple local addresses (192.168.1.0 to 192.168.1.255) to use the same global address. The router retains port numbers to differentiate the connections.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask 255.255.255.240
ip nat inside source list 1 pool net-208 overload
!
interface serial0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

# IP Features NAT

## • Useful NAT command

- **clear ip nat translation \*** - Clear all dynamic address translation entries from the NAT translation table
- **clear ip nat translation inside *global-ip local-ip* [outside *local-ip global-ip*]** - Clear a simple dynamic translation entry containing an inside translation, or both inside and outside translation
- **clear ip nat translation outside *local-ip global-ip*** - Clear a simple dynamic translation entry containing an outside translation
- **show ip nat translations [verbose]** - Display active translations
- **show ip nat statistics** - Display translation statistics

# IP Features DNS

## Dynamic Lookup Example:

```
! IP Domain Name System (DNS)-based host name-to-address translation is enabled
ip domain-lookup
! Specifies host 131.108.1.111 as the primary name server and host 131.108.1.2
! as the secondary server
ip name-server 131.108.1.111 131.108.1.2
! Defines cisco.com as the default domain name the router uses to complete
! unqualified host names
ip domain-name cisco.com
```

# IP Features HSRP

## Hot Standby Router Protocol:

configuration commands followed by an example:

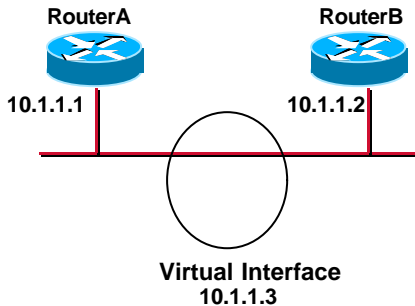
```
! Enables HSRP
standby [<group-number>] ip [<ip-address>] [secondary]]
! Configures the time between hello packets and the hold time before other routers
! declare the active router to be down
standby [<group-number>] timers <hellotime> <holdtime>
! Sets the Hot Standby priority, used in choosing the active router
standby [<group-number>] priority <priority-number>
! Specifies that, if the local router has priority over the current active router,
! the local router should attempt to take its place as the active router
standby [<group-number>] preempt
! Configures the interface to track other interfaces, so that if one of the other interfaces goes
down, the device's Hot Standby priority is lowered
standby [<group-number>] track <type> <number> [<interface-priority>]
```

# IP Features HSRP

Basic example :

```
hostname RouterA
!  
interface ethernet 0  
ip address 10.1.1.1 255.0.0.0  
standby 1 ip 10.1.1.3  
standby 1 preempt  
standby 1 priority 110  
standby 1 timers 5 15
```

```
hostname RouterB  
!  
interface ethernet 0  
ip address 10.1.1.2 255.0.0.0  
standby 1 ip 10.1.1.3  
standby 1 preempt  
standby 1 timers 5 15
```



# IP Features HSRP

HSRP useful commands:

show standby -

RouterA#show standby

Ethernet0 - Group 1

Local state is Active, priority 110, may preempt

Hellotime 5 holdtime 15 configured hellotime 5 sec holdtime 15 sec

Next hello sent in 00:00:02.226

Hot standby IP address is 10.1.1.3 configured

Active router is local

Standby router is 10.5.0.3 expires in 00:00:13

Standby virtual mac address is 0000.0c07.ac01

# IP Features DHCP

Dynamic Host Control Protocol :

DHCP is a protocol that enables you to automatically assign reusable IP addresses to clients

Cisco IOS DHCP server offers the following benefits:

- Reduced Internet access costs
- Simplified IP address management
- Reduced client configuration tasks and costs

Note : DHCP was a new feature in 12.0.(1)T

# IP Features DHCP

DHCP basic example:

**! specifies networkers as the string used for the address pool created**

```
ip dhcp pool networkers  
network 10.1.1.0 255.255.255.0
```

**! Defines a default router**  
**default-router 10.1.1.254**

**! shows a fifteen-minute lease**  
**lease 0 0 15**

# IP Features DHCP

DHCP commands :

**show ip dhcp binding *address*** - Display a list of all bindings created on a specific DHCP server

**show ip dhcp conflict *address*** - Display a list of all address conflicts recorded by a specific DHCP server

**show ip dhcp server statistics** - Display count informaton about server statistics and messges sent and received

**clear ip dhcp binding *address*** - Delete an automatic address binding from the DHCP database

**clear ip dhcp conflict *address*** - Clear an address conflict

# IP Features NTP

Network Time Protocol :

NTP is a protocol designed to time-synchronize a network of machines

Basic example of NTP -

- clock timezone CST -6 - Sets the timezone
- clock summer-time CDT recurring - Configure summer time
- ntp master 3 - Make the system an authoritative NTP server
- ntp update-calander - Configure NTP to update the calendar

# IP Features NTP

NTP useful commands :

**show calendar** - Display the current calendar time

**show clock [detail]** - Display the current system clock time

**show ntp associations [detail]** - Show the status of NTP associations

**show ntp status** - Show the status of NTP

**ntp master [stratum]** - Make the system an authoritative NTP server

**ntp update-calendar** - Configure NTP to update the calendar

# IP Features HTTP

HTTP configuration commands :

**ip http server**- enable any router to be monitored or have its configuration modified from a browser using the Cisco Web browser interface

**ip http port 60**- changes the port from the default of 80



# Questions?