



## NANOG 43 — Brooklyn, NY Wireless and IPv6 Connectivity

### Wireless Network

Wireless Internet service is available in all meeting rooms and many public areas within the meeting space.

Networking at this meeting has been enhanced to create an improved environment for experimenting with and learning about IPv6 connectivity.

### Network setup

Typically the NANOG meeting network offers two wireless LANs (identified by unique SSIDs) that provide dual-stack service; they route traffic for both IPv4 and IPv6 devices, and allow access to all IPv4-based sites as well as to IPv6 sites (for devices that support IPv6). The wireless network for NANOG43 features two additional wireless LANs that will route only IPv6 traffic outside the network. These LANs will be available throughout the meeting so you can experiment with configuring your laptop or other device to operate in this environment.

### Wireless Service Set Identifiers (SSIDs)

The NANOG 43 wireless network features four SSIDs (service set identifiers) to support particular features and optimize performance. Please review the table below for details about each SSID.

| SSID   | General Information   | Addressing  |
|--|---|---|
| <b>Nanog-a</b>                               | If your wireless device supports 802.11a, you will see the SSID <b>nanog-a</b> displayed as an “available network” in your wireless utility, and this SSID will provide the best performance. This SSID is set up <i>only</i> on the .11a interface of the access points. It will not support roaming or hand-over to or from b/g radios. | An IPv4 captive portal gateway is presented at 192.35.164.1, and all wireless addresses are within 192.35.164.0/22. Please do not assign static addresses to devices. |
| <b>Nanog</b>                                 | Choose the SSID <b>nanog</b> if your wireless utility doesn’t detect nanog-a (i.e. your hardware doesn’t support 11a). This SSID is mapped to both .11a and b/g radios in the APs and it supports roaming between .11a and b/g radios. This SSID is generally lower-performing than nanog-a.  | An IPv4 captive portal gateway is presented at 192.35.164.1, and all wireless addresses are within 192.35.164.0/22. Please do not assign static addresses to devices. |
| <b>nanog-v6</b><br>and<br><b>nanog-xp-v6</b> | The SSIDs <b>nanog-v6</b> and <b>nanog-xp-v6</b> are provided to support IPv6 experimentation. Both SSIDs are mapped to both the .11a and b/g radios in the APs.  | Addresses are assigned at the meeting for the following blocks:<br><b>nanog-v6</b><br><b>nanog-xp-v6</b>  |

### Servers

Following are addresses for DNS and SMTP servers on all SSIDs, and a Squid Proxy available on nanog and nanog-a.

| SSID        | Server      | Address                      |
|-------------|-------------|------------------------------|
| nanog-a     | DNS         | 192.35.164.34, 192.35.164.39 |
|             | SMTP        | 192.35.164.37                |
|             | Squid Proxy | 192.35.164.38                |
| Nanog       | DNS         | 192.35.164.34, 192.35.164.39 |
|             | SMTP        | 192.35.164.37                |
|             | Squid Proxy | 192.35.164.38                |
| nanog-v6    | DNS         | 2620:0:CE0:2::42             |
|             | SMTP        | 2620:0:CE0:2::42             |
| nanog-xp-v6 | DNS         | 2620:0:CE0:2::42             |
|             | SMTP        | 2620:0:CE0:2::42             |

### Client Configuration Information

Basic client configuration information for several different operating systems has been collected and is available on the Wiki at:

### **Wireless Cards**

Any 802.11-compatible card of a, b, or g type is supported on the network. You may borrow a PCMCIA 802.11b (Lucent “Hermes”) wireless card to use during the meeting. Cards are available at the registration desk. You will need to show your meeting name badge in order to check out a wireless card and must return the card to the registration desk at the end of meeting. Most current operating systems will have built-in driver support; if you need assistance, please see “Support” below.

### **Wireless Security Reminder**

Please keep in mind that wireless traffic is subject to sniffing and interception. This means that end-to-end encryption (e.g., ssh, IPSEC, https) is crucial to protecting your data and privacy. We recommend the following:

- Use ssh for any terminal connection. If you must connect to a system that doesn't support ssh, at least ssh to an intermediate system to make sure that the portion crossing the local network is encrypted.
- Use scp or sftp instead of non-anonymous ftp; remember that ftp passwords are sent in the clear.
- If using IMAP or POP, configure your mailer to use SSL, or at least APOP.
- If using a web-based interface (e.g., Exchange), make sure to use the “https” URL.
- Remember that any form submission or web password entry may cross the network in the clear.

### **Support**

For assistance, please visit the A/V riser at the back of the ballroom or inquire at the registration desk.